ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	4
Medium	3
Low	6
Informational	0

Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://dev.investorstatelawguide.com/Home/LogPageCountForNotepedUserSession?query=query+AND+1%3D1
Method	GET
Parameter	query
Attack	query 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_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia
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_lcia
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&DocumentL 2&treatycat=
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
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?SearchType=C&id=50&search=ZAP&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_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguag 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_2
Method	GET
Parameter	defendingCountrydisp
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguag 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_2
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&DocumentL
Method	GET
Parameter	treaty_id
Attack	2-2
Instances	10
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 [query AND 1=1] and [query AND 1=2] The parameter value being modified was NOT 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?%20Trading,%20Inc.%20v.%20Democratic%20Republic%20of%20the%20Congo%20(
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?%20Lyle%20Ingredients%20Americas,%20Inc.%20v.%20United%20Mexican%20States
Method	GET
Parameter	disputeId
Attack	515221) 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=dateasc%20%20%20%20%20%23Directory&ID=10&Location=Argentina%25
Method	GET
Parameter	disputeId
Attack	653485) 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)%20an
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?%20Co.%20KG%20(Sweden%20and%20Europe)%20v.%20The%20Federal%20Republ
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?%20Technical%20Cooperative%20Corp.,%20Beijing%20Shougang%20Mining%20Inves
Method	GET
Parameter	disputeId
Attack	1339962) 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?%20Gas%20PLC,%20Poltava%20Hydroelectric%20BV%20v.%20Ukraine%20(SCC%20
Method	GET
Parameter	disputeId
Attack	1143004) 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%252fDisputeDocur
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?%20Machinery%20Ltd.%20v.%20Romania%20(ICSID%20Case%20No.%20ARB/07/13
Method	GET
Parameter	disputeId
Attack	711009) 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.%20Argen
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
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Sons%20Co.%20v.%20Government%20of%20the%20State%20of%20Libya,%20M
Method	GET
Parameter	disputeId
Attack	966601) 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%20v.%20Czech%20Republic&%20Fischer%20GmbH%20&ID=10&Loc
Method	GET
Parameter	disputeId
Attack	1257226) 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%2
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?%20Dominion%20Energy%20Holdings,%20L.P.%20v.%20Dominican%20Republic%20(
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?E%20Capital%20Corp.%20and%20LG&E%20Energy%20Corp.,%20LG&E%20Internati
Method	GET
Parameter	disputeId
Attack	575340) 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%20
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?%20Trust%20(Barbados)%20Ltd.%20v.%20Bolivarian%20Republic%20of%20Venezuel
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?%20Trade%20S.A.%20v.%20Republic%20of%20Turkey%0D%0A(ICSID%20Case%20
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?%20Montenegro%20and%20Republic%20of%20Serbia%20(UNCITRAL)&ID=10&Locat
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?%20Sehil%20Insaat%20Endustri%20ve%20Ticaret%20Ltd.%20Sti.%20v.%20Turkmeni
Method	GET
Parameter	disputeId
Attack	1101688) 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	30
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 oper 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 operatin
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?ID=10&aprule=%3Bsleep+15%3B&aprule_arbrule_lcia_1998=1&aprule_icsid_addfac_1978=1
Method	GET
Parameter	aprule
Attack	;sleep 15;
URL	http://dev.investorstatelawguide.com/ResearchTools/PublicationCitators?SearchTab=%27+++docdataid+++%27%23%27+++docdataid+++%27&cidsp=%27+++docdat
Method	GET
Parameter	toc
Attack	content'|timeout /T 15
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?+Sons+Co.+v.+Government+of+the+State+of+Libya%2C+Ministry+of+Economy+in+the
Method	GET
Parameter	disputeId
Attack	966601"&timeout /T 15&"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_Ge s+15+%23&doccat_7=1&doccat_8=1&hidAccordionIndex=&index=&mainfilter=1%2C2%2C3%2C4%2C5%2C6%2C7%2C8%2C12%2C13%2C15%2C16%2C17%2C1
Method	GET
Parameter	doccat_6
Attack	1;start-sleep -s 15 #
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0003-17%20-%20Waste%20Management%20II%20-%20Mexico%20Subm%20Info.pdf%23navpanes=
Method	GET
Parameter	query

Attack	query';start-sleep -s 15
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=38863&exList=&expandWholeBranchList=38863%27%3Bsleep+15%3B%27&id=50&kwList=
Method	GET
Parameter	expandWholeBranchList
Attack	38863';sleep 15;'
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?PageNumber=97&id=10%3Bstart-sleep+-s+15+%23&sorttab=apptreaty_asc&toc=disputedire
Method	GET
Parameter	id
Attack	10;start-sleep -s 15 #
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia_199 17%2C+Procedural+Order+No.+11%2C+7+June+2018%22%3Bsleep+15%3B%22&toc=disputedirectory&treaty_id=0&treatycat=
Method	GET
Parameter	search
Attack	Michael Ballantine and Lisa Ballantine v. Dominican Republic, PCA Case No. 2016-17, Procedural Order No. 11, 7 June 2018";sleep 15;"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia_1998 17%2C+Procedural+Order+No.+11%2C+7+June+2018&sorttab=apprules_asc&toc=disputedirectory&treaty_id=0&treatycat=
Method	GET
Parameter	hidAccordionIndex
Attack	';sleep 15;'
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0003-24%20Waste%20Management%20II%20-%20WM%20Reply.pdf%23navpanes=0&Page=1?quer
Method	GET
Parameter	query
Attack	query'&sleep 15&'
URL	http://dev.investorstatelawguide.com/start-your-trial?City=ZAP&Country=Albania&Email=ZAP&EnableEditProfile=1&Firm_Institution=ZAP&FirstName=ZAP&I_am_18y
Method	GET
Parameter	active
Attack	0"&timeout /T 15&"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia_1998 17%2C+Procedural+Order+No.+11%2C+7+June+2018&sorttab=apprules_asc&toc=disputedirectory&treaty_id=0&treatycat=
Method	GET
Parameter	aprule_uni_arbrule_2010
Attack	1";start-sleep -s 15
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0003-29%20-%20Waste%20Management%20II%20-%20Mexico%20Add%20Subm.pdf%23navpanes
Method	GET
Parameter	query
Attack	query";sleep 15;"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_Ge
Method	GET
Parameter	doccat_18
Attack	1';sleep 15;'
URL	http://dev.investorstatelawguide.com/ResearchTools/PublicationCitators?SearchTab=%27+++docdataid+++%27%23%27+++docdataid+++%27&cidsp=%27+++docdat
Method	GET
Parameter	docdataid
Attack	' docdataid '&timeout /T 15
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&DocumentL 34%2C+Swiss+Federal+Supreme+Court+Order%2C+23+November+2017+%5BEnglish+Translation%5D&sorttab=apptreaty_asc%22%26sleep+15%26%22&toc=disp
Method	GET
Parameter	sorttab
Attack	apptreaty_asc"&sleep 15&"
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=&docidclose=4632&id=201&subcat=&toc=content%26sleep+15%26
Method	GET
Parameter	toc
Attack	content&sleep 15&
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_Ge
Method	GET
Parameter	doccat_2
Attack	1';sleep 15;'
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0003-19%20-%20Waste%20Management%20II%20-%20PO1%20Doc%20%5BSpanish%5D.pdf%23r
Method	GET
Parameter	query
Attack	query|timeout /T 15
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=regsec%27%3Bstart-sleep+-s+15&toc=mainAnnot
Method	POST
Parameter	cat
Attack	regsec';start-sleep -s 15
Instances	113
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 wh 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 applications, 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 arg 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 If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quo

	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 strir
	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. Reje
	When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs,
	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 indir
	Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide som
	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 attac
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 we 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 privileg 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 containing 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 includ
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_Ge
Method	GET
Parameter	cat
Attack	';alert(1);'
Evidence	';alert(1);'
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia_199
Method	GET
Parameter	toc
Attack	';alert(1);'
Evidence	';alert(1);'
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=&Investme
Method	GET
Parameter	searchType
Attack	javascript:alert(1);
Evidence	javascript:alert(1);
URL	http://dev.investorstatelawguide.com/ResearchTools/JurisprudenceCitators?cidsp=593154&disputeID=593154&id=11&sort=&type=javascript%3Aalert%281%29%3B
Method	GET
Parameter	type
Attack	javascript:alert(1);
Evidence	javascript:alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_Ge
Method	GET
Parameter	aprule
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=investmenttreaty&id=201&subcat=%22+onMouseOver%3D%22alert%281%29%3B&toc=conte
Method	GET
Parameter	subcat
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?Show=y&cat=%22+onMouseOver%3D%22alert%281%29%3B&docid=4632&id=201&subcat=&toc=
Method	GET
Parameter	cat
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/ResearchTools/DTSearchFTS?All_Arbitrator=&All_ArbitratorRules=&All_agreement_id=&All_circDate1=01%2F01%2F1899&All_c
Method	GET
Parameter	All_circDate2
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia_1998
Method	GET
Parameter	toc
Attack	';alert(1);'
Evidence	';alert(1);'
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?id=10&sorttab=apptreaty_desc&toc=%27%3Balert%281%29%3B%27
Method	GET
Parameter	toc
Attack	';alert(1);'
Evidence	';alert(1);'
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=5717&id=201&subcat=%22+onMouseOver%3D%22alert%281%29%3
Method	GET
Parameter	subcat
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia_199
Method	GET

Parameter	index
Attack	';alert(1);'
Evidence	';alert(1);'
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?Global=Yes&cat=%22+onMouseOver%3D%22alert%281%29%3B&id=201&search_title=ZAP&subc
Method	GET
Parameter	cat
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/Home/UserSession
Method	POST
Parameter	HiddenIPAddress
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?SearchType=javascript%3Aalert%281%29%3B&id=50&search=ZAP&tab=r&toc=content
Method	GET
Parameter	SearchType
Attack	javascript:alert(1);
Evidence	javascript:alert(1);
URL	http://dev.investorstatelawguide.com/User/Welcome/TermsPhrases?letter=z&searchType=javascript%3Aalert%281%29%3B&toc=termsPhrases
Method	GET
Parameter	searchType
Attack	javascript:alert(1);
Evidence	javascript:alert(1);
URL	http://dev.investorstatelawguide.com/ResearchTools/TermsPhrases?allText=Y&letter=x&searchTermAgre=ZAP&searchType=javascript%3Aalert%281%29%3B&sorttab
Method	GET
Parameter	searchType
Attack	javascript:alert(1);
Evidence	javascript:alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?PageNumber=97&id=10&sorttab=apptreaty_asc&toc=%27%3Balert%281%29%3B%27
Method	GET
Parameter	toc
Attack	';alert(1);'
Evidence	';alert(1);'
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=%22+onMouseOver%3D%22alert%281%29%
Method	GET
Parameter	DocumentLanguage
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia_1998
Method	GET
Parameter	refresh
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
Instances	135
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 modu 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 co 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-alphanumeric 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 by If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quo 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 c 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 rec 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. Reje When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, 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 moved e
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 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/ResearchTools/ArticleCitator?AgreementID=241&ProvCode=Art2&aaprovid=64574&cat&docid=1295&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=24&ProvCode=ArtXI&aaprovid=31758&cat&docid=67&id=201&sort&subcat&toc=content
Method	GET

Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=134&ProvCode=Art4.(3)&aaprovid=56619&cat&docid=845&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=327&ProvCode=Rule39.A.&aaprovid=73101&cat&docid=1560&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=82&ProvCode=Art37&aaprovid=46578&cat&docid=446&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=110&ProvCode=Art56&aaprovid=51880&cat&docid=809&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=111&ProvCode=Reg14.(3)(a)&aaprovid=56307&cat&docid=842&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=1209&ProvCode=Art42&aaprovid=109406&cat&docid=5132&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=118&ProvCode=Rule49.(1)&aaprovid=54315&cat&docid=819&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=411&ProvCode=Art8.1.&aaprovid=80418&cat&docid=1866&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=125&ProvCode=Rule9.(3)&aaprovid=55392&cat&docid=828&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=73&ProvCode=CommPartIIIChapII&aaprovid=60276&cat&docid=57&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=463&ProvCode=Art8&aaprovid=86450&cat&docid=2112&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=24&ProvCode=ArtXIII&aaprovid=31766&cat&docid=67&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=110&ProvCode=Art16.(2)&aaprovid=51735&cat&docid=809&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=111&ProvCode=Reg22.(2)(b)&aaprovid=56355&cat&docid=842&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=73&ProvCode=(30)&aaprovid=40682&cat&docid=57&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=24&ProvCode=1.&aaprovid=31776&cat&docid=67&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=82&ProvCode=Art19.3.&aaprovid=46510&cat&docid=446&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=73&ProvCode=Art31.(10)&aaprovid=40964&cat&docid=57&id=201&sort&subcat&toc=content
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
Instances	1734
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/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/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/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%2511% 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%27!n%
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%25s
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/SubjectNavigator?ci=46049&id=50&kwList=25889%2C46049&toc=ZAP%25n%25s%25n%25s%25n%25s%25n%
Method	GET
Parameter	toc
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=3806&id=201&subcat=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%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%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/ArticleCitator?cat&docid=3806&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/JurisprudenceCitators?id=11&toc=content&type=gatt
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/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%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 /%s

Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1

Medium (Medium)	**Directory Browsing**
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which can be accessed to read sensitive information.

URL	http://dev.investorstatelawguide.com/highlighter/viewer/locale/
Method	GET
Attack	Parent Directory
Instances	1
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html
CWE Id	548
WASC Id	48
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	http://ocsp.digicert.com/
Method	POST
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)	**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/Treaties/AnnotDocument?agreementID=551&cat=bit&docid=2418&tabcontent&toc=annotSection
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat&docid=2198&id=201&subcat&toc=content
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/documents/documents/IC-0228-33%20-%20Bear%20Creek%20v.%20Peru%20-%20Respondent%20Rejoinder.pdf%23navpanes
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
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/Treaties/AnnotDocument?agreementID=554&cat=bit&tabcontent&toc=annotSection
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=1336&cat=other&docid=2436&tabcontent&toc=annotSection
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=97&cat=other&docid&tabcontent&toc=annotSection
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/documents/documents/AF-0003-10%20-%20Waste%20Management%20II%20-%20PO1%20%5BEnglish%5D.pdf%23navpanes
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/Treaties/AnnotDocument?agreementID=740&cat=bit&docid=2666&tabcontent&toc=annotSection
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=25899&exList&expandWholeBranchList=25899&id=50&kwList=25889,25899,&search&searc
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=1236&cat=bit&docid=5342&tabcontent&toc=annotSection
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=82&id=10&sorttab=scd_asc&toc=disputedirectory
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js

Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
URL	http://dev.investorstatelawguide.com/ResearchTools/FullTextSearch?id=97&selNodeId=46275&tab=r&toc=content
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jqueryui/1.12.1/jquery-ui.min.js" type="text/javascript"></script>
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&DocumentL Mex%2C+LLC+and+others+v.+United+Mexican+States%2C+ICSID+Case+No.+ARB%28AF%29%2F16%2F3%2C+Procedural+Order+No.+4%2C+29+May+2018+&s
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/Treaties/AnnotDocument?agreementID=419&cat=bit&docid=1880&tabcontent&toc=annotSection
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	22738
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)	**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 o content type (if one is set), rather than performing MIME-sniffing.
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=886&cat=other&docid=4114&tabcontent&toc=annotSection
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/highlighter/viewer/?Page=1&file=http://dev.investorstatelawguide.com/documents/documents/BIT-0728%20-%20Belgium-Luxemb
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=589&cat=other&tabcontent&toc=annotSection
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=%252f
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%252fDisputeDoc
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=945&cat=regsec&docid=4210&tabcontent&toc=annotSection
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=nafta&toc=mainAnnot
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=43&cat=bit&tabcontent&toc=annotSection
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&goback=
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/highlighter/viewer/?Page=1&file=http://dev.investorstatelawguide.com/documents/documents/BIT-0223%20-%20Bolivia-Chile%20
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=%252fdisput
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/highlighter/viewer/?Page=1&file=http://dev.investorstatelawguide.com/documents/documents/ARB-0054%20SCC%20Arbitration%
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/Treaties/AnnotDocument?agreementID=465&cat&tabcontent=yes&toc=annotSection
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/highlighter/viewer/?Page=1&file=http://dev.investorstatelawguide.com/documents/documents/NAT-0016%20-%20El%20Salvador
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Honduras%20- %20Astaldi%20S.p.A.%20v.%20Republic%20of%20Honduras%20%5BII%5D%20(ICSID%20Case%20No.%20ARB/07/32)&disputeId=1371348&goback=%252fdisput
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=412&cat=bit&tabcontent&toc=annotSection
Method	GET

Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Kenya%20-%20Cortec%20Mining%20Kenya%20Limited,%20Cortec%20(Pty)%20Limited%20and%20Stirling%20Capital%20Limited%20v.%20Republic%20of%20Kenya%20(ICS
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=43973&exList&expandWholeBranchList=43973&id=50&kwList=26562,43973,&search&searc
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/documents/documents/IC-0070-04_Biwater.pdf
Method	GET
Parameter	X-Content-Type-Options
Instances	15347
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 we
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 browser 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/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Czech%20Republic%20-%20European%20Media%20Ventures%20SA
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Venezuela%20-%20Venezuela%20Holdings%20B.V.%20and%20others%20(formerly%20Mobil%20Corporation%20and%20others)%20v.%20Bolivarian%20Republic%20of%20Venez
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Slovak%20Republic%20-%20European%20American%20Investment%17)&disputeId=1118279&goback=%252fdisputedirectory%252fDisputeDocument%253fPageNumber%253d83%2526id%253d10%2526toc%253ddisputedirectory&pop
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%23na
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Croatia%20-%20MOL%20Hungarian%20Oil%20and%20Gas%20Company%20Plc%20v.%20Republic%20of%20Croatia%20(ICSID%20Case%20No.%20ARB/13/32)&disputeId=1
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%23navpar
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Canada%20-%20Crompton%20(Chemtura)%20Corporation%20v.%20
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=802&toc=annotSection
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=315&cat=other&tabcontent&toc=annotSection
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=1346&cat=other&docid=2446&tabcontent&toc=annotSection
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/documents/documents/IC-0228-14%20-%20Bear%20Creek%20v.%20Peru%20-%20Witness%20Statement%20of%20Zegarra%2
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%23navpanes=0
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(excerpts).p
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/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=6378&id=201&subcat=bit&toc=content
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDoc_AllDocList?ID=10&doclist=AF%2f0035%2f02&goback=%2fdisputedirectory%2fDisputeDocument%3
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?AgreementID=1087&ProvCode=Article%2023&aaprovid=103493&cat&docid=4524&id=201&sort=%
Method	GET
Parameter	X-XSS-Protection

URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Peru%20-%20Bear%20Creek%20Mining%20Corporation%20v.%20Republic%20of%20Peru%20(ICSID%20Case%20No.%20ARB/14/21)&disputeId=1093714&goback=%252fd
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/documents/documents/IC-0239-10%20-%20EuroGas%20v.%20Slovak%20Republic%20-%20PO1.pdf%23navpanes=0&Page=1
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/highlighter/viewer/?Page=1&file=http://dev.investorstatelawguide.com/documents/documents/BIT-0529%20-%20Lesotho-United%
Method	GET
Parameter	X-XSS-Protection
Instances	22262
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 at 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/notepad-login
Method	GET
Parameter	Password
Evidence	Set-Cookie: Password
URL	http://dev.investorstatelawguide.com/User/Welcome/
Method	GET
Parameter	UserCIS
Evidence	Set-Cookie: UserCIS
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	GET
Parameter	UserId
Evidence	Set-Cookie: UserId
Instances	4
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)	**Content-Type Header Missing**
Description	The Content-Type header was either missing or empty.
URL	http://dev.investorstatelawguide.com/highlighter/viewer/locale/locale.properties
Method	GET
Instances	1
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
CWE Id	345
WASC Id	12
Source ID	3