ZAP by Checkmarx Scanning Report

Site: https://demo.testfire.net

Generated on Tue, 6 May 2025 14:31:18

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	4
Low	8
Informational	4

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (DOM Based)	High	1
Absence of Anti-CSRF Tokens	Medium	3
Content Security Policy (CSP) Header Not Set	Medium	198
Missing Anti-clickjacking Header	Medium	82
Secure Pages Include Mixed Content (Including Scripts)	Medium	1
Cookie without SameSite Attribute	Low	3
Cross-Domain JavaScript Source File Inclusion	Low	1
Information Disclosure - Debug Error Messages	Low	1
Secure Pages Include Mixed Content	Low	2
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	296
Strict-Transport-Security Header Not Set	Low	293
Timestamp Disclosure - Unix	Low	2
X-Content-Type-Options Header Missing	Low	126
Information Disclosure - Suspicious Comments	Informational	10
Modern Web Application	Informational	6
Re-examine Cache-control Directives	Informational	83
Session Management Response Identified	Informational	28

Alert Detail

High	Cross Site Scripting (DOM Based)
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 web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. 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 privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. 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 a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. 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 include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	https://demo.testfire.net/login.jsp#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: https://demo.testfire.net/login.jsp<PAYLOAD_0> Write to /html/body/div[1]/form/table/tbody/tr[1]/td[2]/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/form/table/tbody/tr[1]/td[2]/input[1] Access: https://demo.testfire.net/login.jsp<PAYLOAD_0> Write to /html/body/div[1]/form/table/tbody/tr[1]/td[2]/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/form/table/tbody/tr[1]/td[2]/input[2]
Instances	1
	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 module, and Apache Wicket.

Solution	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 components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. 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 characters. 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 bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. 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 choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. 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 recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." 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 elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40026

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://demo.testfire.net/feedback.jsp
Method	GET
Attack	
Evidence	<form name="cmt" method="post" action="sendFeedback">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "cfile" "email_addr" "name" "reset" "subject" "submit"].
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	<form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "btnSubmit" "passw" "uid"].
URL	https://demo.testfire.net/subscribe.jsp
Method	GET
Attack	
Evidence	<form action="doSubscribe" method="post" name="subscribe" id="subscribe" onsubmit=" return confirmEmail(txtEmail.value);">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "btnSubmit" "txtEmail"].
Instances	3
	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.

Solution	For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://demo.testfire.net/altoro/images/gradient.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/default.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/default.jsp?content=security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_deposit.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_careers.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/VoluteeringInformation.pdf
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/feedback.jsp
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/high
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/high_yield_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/icon_top.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_insurance.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_contact.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_insurance.htm

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_careers.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_community.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_executives.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_internships.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_trainee.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061019.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061023.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061024.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061025.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061026.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061027.htm
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060413.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060518.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060720.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060817.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060921.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060928.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061005.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061109.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=privacy.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/inside_points_of_interest.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/grouplife.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_retirement.htm

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_other.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Privacypolicy.jsp?sec=Careers&template=US
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sameDomain
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=AKPwALGz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=fscfvjGd
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/search.jsp?query=HaXLuZFt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=hOnhqNiD
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=IkOZiNXz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=JAAQMvLJ
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=jpWbwjcT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=mXyQatmo
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=SzEmnVIq
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/search.jsp?query=UDMIAKJd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=uXRWmkhy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=xIJnMfQg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/status_check.jsp

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=a
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=b
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=c
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=vxgVjbxx
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=email
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonaCJFvyhA
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonAqLXrWwB
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonCFoGkQSB
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonFDSRDpSD
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonJBFhDQoT
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonouQoStlr
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonpZXRDHBW
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsontktUEjVp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonvSygygvR
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonwmmLvaDL
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonWvLjXPcIFXDqOOto
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonxSYIqVJjeBBZJfaf
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sendFeedback
Method	POST
Attack	
Evidence	
Other Info	
Instances	198
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/feedback.jsp
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/high_yield_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_community.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_executives.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_internships.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_trainee.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061019.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061023.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061024.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061025.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061026.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061027.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060413.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=pr/20060518.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060720.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060817.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060921.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060928.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061005.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061109.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=privacy.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=AKPwALGz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=fscfvjGd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=HaXLuZFt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=hOnhqNiD
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=IkOZiNXz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=JAAQMvLJ
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=jpWbwjcT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=mXyQatmo
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=SzEmnVIq
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=UDMIAKJd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=uXRWmkhy
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/search.jsp?query=xIJnMfQg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/status_check.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=a
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=b
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=c

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=vxgVjbxx
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=email
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sendFeedback
Method	POST
Attack	
Evidence	
Other Info	
Instances	82
	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

Solution	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	Secure Pages Include Mixed Content (Including Scripts)
Description	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	http://demo-analytics.testfire.net/urchin.js
Other Info	tag=script src=http://demo-analytics.testfire.net/urchin.js
Instances	1
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
CWE Id	311
WASC Id	4
Plugin Id	10040

Low	Cookie without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	Set-Cookie: JSESSIONID
Other Info	
URL	https://demo.testfire.net/robots.txt
Method	GET
Attack	
Evidence	Set-Cookie: JSESSIONID
Other Info	
URL	https://demo.testfire.net/sitemap.xml
Method	GET

Attack	
Evidence	Set-Cookie: JSESSIONID
Other Info	
Instances	3
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	<script src="http://demo-analytics.testfire.net/urchin.js" type="text/javascript"> </script>
Other Info	
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
Plugin Id	10017

Low	Information Disclosure - Debug Error Messages
Description	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.
URL	https://demo.testfire.net/swagger/properties.json
Method	GET
Attack	
Evidence	Internal server error
Other Info	
Instances	1
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	1295
WASC Id	13
Plugin Id	10023

Low	Secure Pages Include Mixed Content
Description	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.

URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	http://www.exampledomainnotinuse.org/mybeacon.gif
Other Info	tag=img src=http://www.exampledomainnotinuse.org/mybeacon.gif
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0
Other Info	tag=object codebase=http://fpdownload.macromedia.com/pub/shockwave/cabs/flash /swflash.cab#version=6,0,0,0
Instances	2
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
CWE Id	311
WASC Id	4
Plugin Id	10040

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://demo.testfire.net/admin/clients.xls
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/altoro/images/gradient.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/api/account/aUULBOtp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/AUvgghWU
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/AUvgghWUHCoOAILd
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/AUvgghWUHCoOAILdDHzDqEKI
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/KBBNLvgJ/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/KBBNLvgJlFQhaIiN/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkg/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkggPfjAHto/transactions
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkggPfjAHtonniCKqDw/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkggPfjAHtonniCKqDwHWwhVcHA/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkgqFqiEBHYBGWjlRtB/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkgqFqiEBHYBGWjlRtBqLsOoJCo/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkgqFqiEBHYBGWjlRtBqLsOoJCoLRJbEoGG/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMy
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMyPeBBZgcHTHdPsrwbsZSmTaKl
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMyPeBBZgcHvRWhGoeS
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMyXHbbtbFe
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/NUzXafXQ/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/NUzXafXQfgrcpWTp/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/NUzXafXQyxMfnbzPvYLnOqAP/transactions
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/ummQDNRX
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/WbCPRCwn
Method	GET
Attack	
Evidence	Apache-Coyote/1.1

Other Info	
URL	https://demo.testfire.net/api/account/WbCPRCwnAfyFmeQi
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/heKyDKFs
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfL
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLPTSLxsjc
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLPTSLxsjchlaQZCKL
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLPTSLxsjchlaQZCKLRVFLgEhK
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLTcEXnLUJkZocEzvV
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/api/feedback/iVlmSagL
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/qbCCyYns
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/ZhPgoSZM
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/ZhPgoSZMGhLSZYyW
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/ZhPgoSZMGhLSZYyWtthJLHFz
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/login
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/logout
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/cgi.exe
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/default.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/default.jsp?content=security.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/cgi.exe
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_cards.htm
Method	GET
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other	

Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_deposit.htm

Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/subscribe.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/VoluteeringInformation.pdf
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/favicon.ico
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/feedback.jsp
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/high
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/high_yield_investments.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/adobe.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/altoro.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/b_cards.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/b_deposit.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/b_insurance.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1

Other Info	
URL	https://demo.testfire.net/images/b_lending.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/b_main.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/b_other.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/b_retirement.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/cancel.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/cgi.exe
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/gradient.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/images/header_pic.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/home1.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/home2.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/home3.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/icon_top.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_deposit.htm
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_careers.htm
Method	GET
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other	

Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/inside1.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/inside3.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/inside4.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/inside5.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/inside6.jpg

Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/inside7.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/logo.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/ok.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_cards.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_checking.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_deposit.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_investments.jpg
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_loans.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_main.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/p_other.jpg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/pf_lock.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/spacer.gif
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/images/subscribe.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1

Other Info	
URL	https://demo.testfire.net/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_community.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_executives.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_internships.htm
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement

Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_trainee.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061019.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061023.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061024.htm
Method	GET
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061025.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061026.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061027.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1

Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_savings.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060413.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060518.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060720.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/index.jsp?content=pr/20060817.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060921.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060928.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061005.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061109.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=privacy.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/index.jsp?content=security.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/inside_points_of_interest.htm
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/cgi.exe
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/grouplife.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_insurance.htm

Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other	

Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_deposit.htm
Method	GET
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/subscribe.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/pr/communityannualreport.pdf
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/Privacypolicy.jsp?sec=Careers&template=US
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/retirement.htm
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/robots.txt
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/sameDomain
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=AKPwALGz
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=fscfvjGd
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=HaXLuZFt
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=hOnhqNiD
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=IkOZiNXz
Method	GET
Attack	
Evidence	Apache-Coyote/1.1

Other Info	
URL	https://demo.testfire.net/search.jsp?query=JAAQMvLJ
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=jpWbwjcT
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=mXyQatmo
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=SzEmnVIq
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=UDMIAKJd
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=uXRWmkhy
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/search.jsp?query=xIJnMfQg
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/search.jsp?query=ZAP
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/security.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/sitemap.xml
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/cgi.exe
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_insurance.htm
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_contact.htm
Method	GET
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other	

Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/personal_savings.htm
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/static/subscribe.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/status_check.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/style.css
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/subscribe.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/subscribe.swf

Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=a
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=b
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=c
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=d
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=vxgVjbxx
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=email
Method	GET

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/favicon-16x16.png
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/favicon-32x32.png
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.json
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonaCJFvyhA
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonAqLXrWwB
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonCFoGkQSB
Method	GET
Attack	
Evidence	Apache-Coyote/1.1

Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonFDSRDpSD
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonJBFhDQoT
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonouQoStlr
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonpZXRDHBW
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsontktUEjVp
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonvSygygvR
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonwmmLvaDL
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	

URL	https://demo.testfire.net/swagger/properties.jsonWvLjXPcIFXDqOOto
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonxSYIqVJjeBBZJfaf
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/swagger/swagger-ui.css
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
Method	GET
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/BnPeVrBJybfHsCNd/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/doEEcrkOKnQCHaGQ/transactions
Method	POST

Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/HiIKVNNW/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/lzVFLnzpkJgcBqNPHXzSWrJD/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/MsEqzATi/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/OAAEQzRP/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/VhzeQSbR/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/YmSbhglK/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/YUpPfUqA/transactions
Method	POST
Attack	

Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/zsvaeHXB/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/zsvaeHXBsNsjkdno/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/account/zsvaeHXBvTmXYrSgTmBaymUt/transactions
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/admin/addUser
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/admin/changePassword
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/feedback/submit
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/api/login
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other	

Info	
URL	https://demo.testfire.net/api/transfer
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/doLogin
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/doSubscribe
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
URL	https://demo.testfire.net/sendFeedback
Method	POST
Attack	
Evidence	Apache-Coyote/1.1
Other Info	
Instances	296
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://demo.testfire.net/altoro/images/gradient.jpg
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/api/account
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/aUULBOtp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/AUvgghWU
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/AUvgghWUHCoOAILd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/AUvgghWUHCoOAILdDHzDqEKI
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/KBBNLvgJ/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/KBBNLvgJlFQhaIiN/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkg/transactions
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkggPfjAHto/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkggPfjAHtonniCKqDw/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkggPfjAHtonniCKqDwHWwhVcHA/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkgqFqiEBHYBGWjlRtB/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkgqFqiEBHYBGWjlRtBqLsOoJCo/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MGOygMkgqFqiEBHYBGWjlRtBqLsOoJCoLRJbEoGG/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMy
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMyPeBBZgcHTHdPsrwbsZSmTaKl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMyPeBBZgcHvRWhGoeS
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MWnwcfMyXHbbtbFe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/NUzXafXQ/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/NUzXafXQfgrcpWTp/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/NUzXafXQyxMfnbzPvYLnOqAP/transactions
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/ummQDNRX
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/api/account/WbCPRCwn
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/WbCPRCwnAfyFmeQi
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/heKyDKFs
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfL
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLPTSLxsjc
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLPTSLxsjchlaQZCKL
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/hQOuYQfLPTSLxsjchlaQZCKLRVFLgEhK
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/api/feedback/hQOuYQfLTcEXnLUJkZocEzvV
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/iVlmSagL
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/qbCCyYns
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/ZhPgoSZM
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/ZhPgoSZMGhLSZYyW
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/ZhPgoSZMGhLSZYyWtthJLHFz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/logout
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/default.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/default.jsp?content=security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_checking.htm

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Documents/JohnSmith/VoluteeringInformation.pdf
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/favicon.ico
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/feedback.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/high
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/high_yield_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/adobe.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/altoro.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/b_cards.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/b_deposit.jpg
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/images/b_insurance.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/b_lending.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/b_main.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/b_other.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/b_retirement.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/cancel.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/images/gradient.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/header_pic.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/home1.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/home2.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/home3.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/icon_top.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_cards.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_about.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/inside1.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/inside3.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/inside4.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/inside5.jpg

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/inside6.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/inside7.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/logo.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/ok.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_cards.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_checking.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_deposit.jpg
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_investments.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_loans.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_main.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/p_other.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/pf_lock.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/spacer.gif
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/images/subscribe.jsp
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/index.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_community.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_executives.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_internships.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_trainee.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061019.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061023.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061024.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061025.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061026.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061027.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060413.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060518.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=pr/20060720.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060817.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060921.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060928.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061005.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061109.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=privacy.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=security.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/inside_points_of_interest.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/grouplife.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_deposit.htm

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_checking.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/pr/communityannualreport.pdf
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/Privacypolicy.jsp?sec=Careers&template=US
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sameDomain
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=AKPwALGz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=fscfvjGd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=HaXLuZFt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=hOnhqNiD
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/search.jsp?query=IkOZiNXz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=JAAQMvLJ
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=jpWbwjcT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=mXyQatmo
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=SzEmnVIq
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=UDMIAKJd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=uXRWmkhy
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/search.jsp?query=xIJnMfQg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/cgi.exe
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_deposit.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_careers.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/static/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/status_check.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/subscribe.jsp

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/subscribe.swf
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=a
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=b
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=c
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=vxgVjbxx
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=email
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/favicon-16x16.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonaCJFvyhA
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonAqLXrWwB
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonCFoGkQSB
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonFDSRDpSD
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonJBFhDQoT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonouQoStlr
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonpZXRDHBW
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsontktUEjVp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonvSygygvR
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/swagger/properties.jsonwmmLvaDL
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonWvLjXPcIFXDqOOto
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.jsonxSYIqVJjeBBZJfaf
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/swagger-ui.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/BnPeVrBJybfHsCNd/transactions
Method	POST

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/doEEcrkOKnQCHaGQ/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/HiIKVNNW/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/IzVFLnzpkJgcBqNPHXzSWrJD/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/MsEqzATi/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/OAAEQzRP/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/VhzeQSbR/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/YmSbhglK/transactions
Method	POST
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/YUpPfUqA/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/zsvaeHXB/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/zsvaeHXBsNsjkdno/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/account/zsvaeHXBvTmXYrSgTmBaymUt/transactions
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/admin/addUser
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/admin/changePassword
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/feedback/submit
Method	POST
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/api/login
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/api/transfer
Method	POST
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/sendFeedback
Method	POST
Attack	
Evidence	
Other Info	
Instances	293
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Method	GET
Attack	
Evidence	1431655765
Other Info	1431655765, which evaluates to: 2015-05-15 04:09:25.
URL	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Method	GET
Attack	
Evidence	1431655765
Other Info	1431655765, which evaluates to: 2015-05-15 04:09:25.

Instances	2
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**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://demo.testfire.net/api/logout
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/feedback.jsp
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/high_yield_investments.htm
Method	GET

Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/adobe.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/altoro.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_cards.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_deposit.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_insurance.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_lending.jpg
Method	GET
Attack	

Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_main.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_other.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/b_retirement.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/cancel.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/gradient.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/header_pic.jpg
Method	GET
Attack	

Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/home1.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/home2.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/home3.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/inside1.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/inside3.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/inside4.jpg
Method	GET
Attack	
Evidence	

Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/inside5.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/inside6.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/inside7.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/logo.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/ok.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_cards.jpg
Method	GET
Attack	
Evidence	

Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_checking.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_deposit.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_investments.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_loans.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_main.jpg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/p_other.jpg
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/pf_lock.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/images/spacer.gif
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client

	or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_community.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_executives.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_internships.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.

URL	https://demo.testfire.net/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_trainee.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=jobs/20061019.htm
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=jobs/20061023.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=jobs/20061024.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=jobs/20061025.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=jobs/20061026.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=jobs/20061027.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client

	or server error responses.
URL	https://demo.testfire.net/index.jsp?content=personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20060413.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20060518.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20060720.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20060817.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20060921.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.

URL	https://demo.testfire.net/index.jsp?content=pr/20060928.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20061005.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=pr/20061109.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=privacy.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/index.jsp?content=security.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.

URL	https://demo.testfire.net/pr/communityannualreport.pdf
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/retirement.htm
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=AKPwALGz
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=fscfvjGd
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=HaXLuZFt
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=hOnhqNiD
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=IkOZiNXz

Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=JAAQMvLJ
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=jpWbwjcT
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=mXyQatmo
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=SzEmnVIq
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=UDMIAKJd
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=uXRWmkhy

Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=xIJnMfQg
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/search.jsp?query=ZAP
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/status_check.jsp
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/style.css
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/subscribe.swf
Method	GET

Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp?step=a
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp?step=b
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp?step=c
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp?step=d
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=vxgVjbxx
Method	GET

Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/survey_questions.jsp?step=email
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/favicon-16x16.png
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/properties.json
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Method	GET
Attack	

Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/swagger/swagger-ui.css
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
Method	GET
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/api/feedback/submit
Method	POST
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/api/login
Method	POST
Attack	
Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
URL	https://demo.testfire.net/sendFeedback
Method	POST
Attack	

Evidence	
Other Info	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 scan rule will not alert on client or server error responses.
Instances	126
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
	https://demo.testfire.net/index.jsp?content=inside_jobs.

URL	htm&job=MortgageLendingAccountExecutive:Sales
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "/* tell the user the job isn't open anymore */", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/swagger/swagger-ui-bundle.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//facebook.github.io/react/docs/error-decoder.html?invariant="+e,r=0;r<t;r++)n+="&args[]="+encodeURIComponent(arguments[r+1]);n+", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/swagger/swagger-ui-standalone-preset.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//","#"==f][--p];);l+=f}}(t)},e.mapToList=function t(e){var n=arguments.length>1&&void 0!==arguments[1]?arguments[1]:"key";var r", see evidence field for the suspicious comment/snippet.
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "<!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->", see evidence field for the suspicious comment/snippet.
Instances	10
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615

WASC Id	13
Plugin Id	10027

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	<a href="#" onclick="go();return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0" ></a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	<a href="#" onclick="go();return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0" ></a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	<a href="">Altoro Private Bank</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	<a name="gift"></a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	<a href="">Altoro Private Bank</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	<script src="./swagger-ui-bundle.js"> </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	6

Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://demo.testfire.net/api/logout
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.microsoft.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/feedback.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/high_yield_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/index.jsp?content=business.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_deposit.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_insurance.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_lending.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=business_retirement.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=inside.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_about.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_benefits.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_careers.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_community.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_contact.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_executives.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_internships.htm
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_investor.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=CustomerServiceRepresentative:CustomerService
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=LoyaltyMarketingProgramManager:Marketing
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=MortgageLendingAccountExecutive:Sales
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_press.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_trainee.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=inside_volunteering.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061019.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061023.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061024.htm
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061025.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061026.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=jobs/20061027.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_cards.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_checking.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Method	GET
Attack	
Evidence	

Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_investments.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_loans.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_other.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=personal_savings.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060413.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060518.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060720.htm
Method	GET
Attack	
Evidence	
Other Info	

URL	https://demo.testfire.net/index.jsp?content=pr/20060817.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060921.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20060928.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061005.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=pr/20061109.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=privacy.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/index.jsp?content=security.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/login.jsp
Method	GET

Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/retirement.htm
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=AKPwALGz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=fscfvjGd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=HaXLuZFt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=hOnhqNiD
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=IkOZiNXz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=JAAQMvLJ
Method	GET
Attack	

Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=jpWbwjcT
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=mXyQatmo
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=SzEmnVIq
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=UDMIAKJd
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=uXRWmkhy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=xIJnMfQg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/search.jsp?query=ZAP
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://demo.testfire.net/status_check.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/subscribe.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=a
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=b
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=c
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=vxgVjbxx

Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/survey_questions.jsp?step=email
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/swagger/properties.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://demo.testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual
Method	GET
Attack	
Evidence	
Other Info	
Instances	83
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	011B6866717FB11D61F3F30595F3B7E2
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	19BB9B8454C033821EAFB3D25659C3F5
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	36F3D22DCCB012038B707CCA7EF4EC17
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	3A1AE7CAF34CD15728355B28E40288FF
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	6E60796C70F2F7759A3A2278D7A495E4
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	6F8F83F39C4623334BC89BD68C3C2B46
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	771A0DE3C82274924A0D72779C4FAB89
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET

Attack	
Evidence	A8A23A1542E06FA6EBC1F79BA8C2A3D7
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	C0AF9AB2C7625CC3979B58C78D9FE586
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	C1256C5CFC348170C43097643812189D
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	C130EFCF9E43BE1875944D2AE012E80A
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	E4338D3474195FB7DB163452E7FBE6F8
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	F477B78123A26C3122F85F6C446CDA9B
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	FAAC78C2B6E6511B6EBA65B8C19BFEB1
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/robots.txt
Method	GET
Attack	

Evidence	56A244F4C5B59B44BECFFAA824794889
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/sitemap.xml
Method	GET
Attack	
Evidence	81981FBF1E09D8D8C04874906B88175D
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	011B6866717FB11D61F3F30595F3B7E2
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	19BB9B8454C033821EAFB3D25659C3F5
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	36F3D22DCCB012038B707CCA7EF4EC17
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	6E60796C70F2F7759A3A2278D7A495E4
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	6F8F83F39C4623334BC89BD68C3C2B46
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	771A0DE3C82274924A0D72779C4FAB89
Other	

Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	A8A23A1542E06FA6EBC1F79BA8C2A3D7
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	C1256C5CFC348170C430976438121890
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	C130EFCF9E43BE1875944D2AE012E80A
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	F477B78123A26C3122F85F6C446CDA9B
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/login.jsp
Method	GET
Attack	
Evidence	FAAC78C2B6E6511B6EBA65B8C19BFEB1
Other Info	cookie:JSESSIONID
URL	https://demo.testfire.net/robots.txt
Method	GET
Attack	
Evidence	56A244F4C5B59B44BECFFAA824794889
Other Info	cookie:JSESSIONID
Instances	28
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112