ZAP Scanning Report

Sites: https://google-gruyere.appspot.com http://google-gruyere.appspot.com

Generated on Tue, 6 Feb 2024 11:52:22

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	3
Low	4
Informational	8

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (Reflected)	High	1
Absence of Anti-CSRF Tokens	Medium	8
Content Security Policy (CSP) Header Not Set	Medium	75
Missing Anti-clickjacking Header	Medium	73
Cookie No HttpOnly Flag	Low	3
Cookie without SameSite Attribute	Low	3
Strict-Transport-Security Header Not Set	Low	28
X-Content-Type-Options Header Missing	Low	93
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	12
Cookie Poisoning	Informational	4
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	19
Re-examine Cache-control Directives	Informational	17
Retrieved from Cache	Informational	3
Session Management Response Identified	Informational	19
User Agent Fuzzer	Informational	48

Alert Detail

High	Cross Site Scripting (Reflected)
	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

Description	/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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/snippets.gtl?uid=%3C%2Fh2%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Ch2%3E
Method	GET
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
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. 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.

Solution	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	40012

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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	<form method='get' action='/382665580745386307547168512335551204731/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] was found in the following HTML form: [Form 1: "pw" "uid"].
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	<form method='get' action='/382665580745386307547168512335551204731/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] was found in the following HTML form: [Form 1: "pw" "uid"].
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	<form method='get' action='/382665580745386307547168512335551204731/saveprofile'>
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] was found in the following HTML form: [Form 1: "action" "is_author" "pw" "uid"].
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login
Method	GET
Attack	
Evidence	<form method='get' action='/397587545265662818066921574239585949762/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] was found in the following HTML form: [Form 1: "pw" "uid"].
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	<form method='get' action='/397587545265662818066921574239585949762/login'>
Other	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,

Info	_csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "pw" "uid"].
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/newaccount.gtl
Method	GET
Attack	
Evidence	<form method='get' action='/397587545265662818066921574239585949762/saveprofile'>
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] was found in the following HTML form: [Form 1: "action" "is_author" "pw" "uid"].
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	<form method='get' action='/382665580745386307547168512335551204731/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] was found in the following HTML form: [Form 1: "pw" "uid"].
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	<form method='get' action='/382665580745386307547168512335551204731/saveprofile'>
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] was found in the following HTML form: [Form 1: "action" "is_author" "pw" "uid"].
Instances	8
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. 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	http://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/0
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/3
Method	GET

Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/snippets.gtl?uid=cheddar

Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	
Other Info	
	http://google-gruyere.appspot.com/397587545265662818066921574239585949762

URL	/snippets.gtl?uid=cheddar
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/6
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/7
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/8
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/9
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/
Method	GET

Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?data.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?gruyere.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?gtl.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resoources/dump.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/dump.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/editprofile.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/error.gtl
Method	GET
Attack	

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/feed.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/home.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/manage.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/menubar.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?sanitize.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/data.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/gruyere.py
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://google-gruyere.appspot.com/code/gtl.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/dump.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/editprofile.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/error.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/feed.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/home.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/manage.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/menubar.gtl

Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/sanitize.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/start
Method	GET

Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/static/codeindex/html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/feed.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	

Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/quitserver.
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/RESET.
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True&uid=username
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/code/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part2
Method	GET

Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/codeindex/html
Method	GET
Attack	
Evidence	
Other Info	
Instances	75
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy

Reference	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 include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/0
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/snippets.gtl?uid=cheddar
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET

Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/snippets.gtl?uid=cheddar
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/4

Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/6
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/7
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/8
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/9
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?data.py
Method	GET
Attack	

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?gruyere.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?gtl.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resoources/dump.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/dump.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/editprofile.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/error.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/feed.gtl
Method	GET
Attack	
Evidence	

Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/home.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/manage.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?resources/menubar.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/?sanitize.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/data.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/gruyere.py
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/gtl.py
Method	GET
Attack	
Evidence	
Other Info	

URL	http://google-gruyere.appspot.com/code/resources/dump.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/editprofile.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/error.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/feed.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/home.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/manage.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/resources/menubar.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/code/sanitize.py
Method	GET

Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	

Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/feed.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/quitserver.
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/RESET.
Method	GET
Attack	

Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True&uid=username
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/code/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part4
Method	GET
Attack	

Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	
Evidence	
Other Info	
Instances	73
Solution	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. 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

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP

Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE
Other Info	
URL	http://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE_ID
Other Info	
Instances	3
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE
Other Info	
URL	http://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE_ID
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	**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://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/%C9%A1ru%CB%90%CB%88j%C9%9B%C9%99r/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/feed.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	

URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/quitserver.
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/RESET.
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True&uid=username
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/code/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/gruyere-code.zip
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/gruyere-code.zip.
Method	GET
Attack	
Evidence	
Other Info	

URL	https://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/start.
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/cheese_b.png

Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/cheese_bw.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/cheese_w.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/codeindex/html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/codelab.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/gruyere-78.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/static/gruyere.png
Method	GET
Attack	

Evidence	
Other Info	
Instances	28
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	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://google-gruyere.appspot.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	http://google-gruyere.appspot.com/0
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	http://google-gruyere.appspot.com/1
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	http://google-gruyere.appspot.com/2
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	http://google-gruyere.appspot.com/3
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/lib.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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login?pw=ZAP&uid=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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/snippets.gtl?uid=brie
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/snippets.gtl?uid=cheddar
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/lib.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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login

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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/newaccount.gtl
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/snippets.gtl?uid=brie
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/snippets.gtl?uid=cheddar
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	http://google-gruyere.appspot.com/4
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	http://google-gruyere.appspot.com/5
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	http://google-gruyere.appspot.com/6
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	http://google-gruyere.appspot.com/7
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	http://google-gruyere.appspot.com/8
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	http://google-gruyere.appspot.com/9
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	http://google-gruyere.appspot.com/code/
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	http://google-gruyere.appspot.com/code/?data.py
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	http://google-gruyere.appspot.com/code/?gruyere.py
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	http://google-gruyere.appspot.com/code/?gtl.py
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	http://google-gruyere.appspot.com/code/?resoources/dump.gtl
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	http://google-gruyere.appspot.com/code/?resources/dump.gtl
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	http://google-gruyere.appspot.com/code/?resources/editprofile.gtl
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	http://google-gruyere.appspot.com/code/?resources/error.gtl
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	http://google-gruyere.appspot.com/code/?resources/feed.gtl
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	http://google-gruyere.appspot.com/code/?resources/home.gtl
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	http://google-gruyere.appspot.com/code/?resources/manage.gtl
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	http://google-gruyere.appspot.com/code/?resources/menubar.gtl
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	http://google-gruyere.appspot.com/code/?sanitize.py
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	http://google-gruyere.appspot.com/code/data.py
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	http://google-gruyere.appspot.com/code/gruyere.py
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	http://google-gruyere.appspot.com/code/gtl.py
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	http://google-gruyere.appspot.com/code/resources/dump.gtl
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	http://google-gruyere.appspot.com/code/resources/editprofile.gtl
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	http://google-gruyere.appspot.com/code/resources/error.gtl

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	http://google-gruyere.appspot.com/code/resources/feed.gtl
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	http://google-gruyere.appspot.com/code/resources/home.gtl
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	http://google-gruyere.appspot.com/code/resources/manage.gtl
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	http://google-gruyere.appspot.com/code/resources/menubar.gtl
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	http://google-gruyere.appspot.com/code/sanitize.py
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	http://google-gruyere.appspot.com/gruyere-code.zip

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	http://google-gruyere.appspot.com/part1
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	http://google-gruyere.appspot.com/part2
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	http://google-gruyere.appspot.com/part3
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	http://google-gruyere.appspot.com/part4
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	http://google-gruyere.appspot.com/part5
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	http://google-gruyere.appspot.com/robots.txt
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	http://google-gruyere.appspot.com/start
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	http://google-gruyere.appspot.com/static/cheese_b.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	http://google-gruyere.appspot.com/static/cheese_bw.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	http://google-gruyere.appspot.com/static/cheese_w.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	http://google-gruyere.appspot.com/static/closed.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	http://google-gruyere.appspot.com/static/codeindex.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	http://google-gruyere.appspot.com/static/codelab.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	http://google-gruyere.appspot.com/static/gruyere-40.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	http://google-gruyere.appspot.com/static/gruyere-78.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	http://google-gruyere.appspot.com/static/gruyere-badge.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	http://google-gruyere.appspot.com/static/gruyere.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://google-gruyere.appspot.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://google-gruyere.appspot.com/382665580745386307547168512335551204731/
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://google-gruyere.appspot.com/382665580745386307547168512335551204731/feed.gtl
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://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
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://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
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://google-gruyere.appspot.com/382665580745386307547168512335551204731/quitserver.
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://google-gruyere.appspot.com/382665580745386307547168512335551204731/RESET.

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://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True
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://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True&uid=username
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://google-gruyere.appspot.com/code/
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://google-gruyere.appspot.com/gruyere-code.zip
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://google-gruyere.appspot.com/part1
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://google-gruyere.appspot.com/part2
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://google-gruyere.appspot.com/part3
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://google-gruyere.appspot.com/part4
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://google-gruyere.appspot.com/part5
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://google-gruyere.appspot.com/start
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://google-gruyere.appspot.com/static/cheese_b.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://google-gruyere.appspot.com/static/cheese_bw.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://google-gruyere.appspot.com/static/cheese_w.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://google-gruyere.appspot.com/static/codeindex.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://google-gruyere.appspot.com/static/codelab.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://google-gruyere.appspot.com/static/gruyere-78.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://google-gruyere.appspot.com/static/gruyere.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.
Instances	93

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	**Charset Mismatch (Header Versus Meta Content-Type Charset)**
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	http://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	http://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	http://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	http://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	http://google-gruyere.appspot.com/part4
Method	GET

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	http://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	https://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	https://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	https://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	https://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	https://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
URL	https://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	

Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [utf-8] and [ISO-8859-1] do not match.
Instances	12
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	**Cookie Poisoning**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where cookie parameters might be controlled. This is called a cookie poisoning attack, and becomes exploitable when an attacker can manipulate the cookie in various ways. In some cases this will not be exploitable, however, allowing URL parameters to set cookie values is generally considered a bug.
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP User-input was found in the following cookie: GRUYERE=26087470|ZAP||author; path=/382665580745386307547168512335551204731 The user input was: pw=ZAP
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP User-input was found in the following cookie: GRUYERE=26087470|ZAP||author; path=/382665580745386307547168512335551204731 The user input was: uid=ZAP
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP User-input was found in the following cookie: GRUYERE=26087470|ZAP||author; path=/397587545265662818066921574239585949762 The user input was: pw=ZAP
	http://google-gruyere.appspot.com/397587545265662818066921574239585949762

URL	/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://google-gruyere.appspot.com /397587545265662818066921574239585949762/saveprofile? action=new&is_author=True&pw=ZAP&uid=ZAP User-input was found in the following cookie: GRUYERE=26087470|ZAP||author; path= /397587545265662818066921574239585949762 The user input was: uid=ZAP
Instances	4
Solution	Do not allow user input to control cookie names and values. If some query string parameters must be set in cookie values, be sure to filter out semicolon's that can serve as name/value pair delimiters.
Reference	https://en.wikipedia.org/wiki/HTTP_cookie https://cwe.mitre.org/data/definitions/565.html
CWE Id	565
WASC Id	20
Plugin Id	10029

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/lib.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " * Processes refresh response {'private_snippet':snippet, user:snippet, ...}", see evidence field for the suspicious comment/snippet.
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/lib.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " * Processes refresh response {'private_snippet':snippet, user:snippet, ...}", see evidence field for the suspicious comment/snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
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	http://google-gruyere.appspot.com/

Method	GET
Attack	
Evidence	<A name="0__hackers"></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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	Refresh
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731 /snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	Refresh
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	http://google-gruyere.appspot.com/382665580745386307547168512335551204731 /snippets.gtl?uid=cheddar
Method	GET
Attack	
Evidence	Refresh
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	
Evidence	Refresh
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762 /snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	Refresh
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	http://google-gruyere.appspot.com/397587545265662818066921574239585949762 /snippets.gtl?uid=cheddar
Method	GET
Attack	

Evidence	Refresh
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	http://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	<A name="1__setup"> </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	http://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	<A name="2__cross_site_scripting"> </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	http://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	<A name="3__client_state_manipulation"> </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	http://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	<A name="4__path_traversal"> </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	http://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	<A name="5__configuration_vulnerabilities"> </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://google-gruyere.appspot.com/
Method	GET
Attack	
Evidence	<A name="0__hackers"></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://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	Refresh

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://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	<A name="1__setup"> </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://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	<A name="2__cross_site_scripting"> </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://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	<A name="3__client_state_manipulation"> </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://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	<A name="4__path_traversal"> </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://google-gruyere.appspot.com/part5
Method	GET
Attack	
Evidence	<A name="5__configuration_vulnerabilities"> </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.
Instances	19
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://google-gruyere.appspot.com/

Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/feed.gtl
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/newaccount.gtl
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/quitserver.
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/RESET.
Method	GET
Attack	
Evidence	no-cache
Other Info	
	https://google-gruyere.appspot.com/382665580745386307547168512335551204731

URL	/saveprofile?action=update&is_admin=True
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True&uid=username
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/code/
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/part1
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/part2
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/part3
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/part4
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/part5

Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/start
Method	GET
Attack	
Evidence	no-cache
Other Info	
URL	https://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	
Evidence	public, max-age=600
Other Info	
Instances	17
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	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	http://google-gruyere.appspot.com/static/cheese_b.png
Method	GET
Attack	
Evidence	Age: 238
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	http://google-gruyere.appspot.com/static/cheese_w.png
Method	GET
Attack	
Evidence	Age: 237
Other	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is

Info	in use.
URL	http://google-gruyere.appspot.com/static/gruyere.png
Method	GET
Attack	
Evidence	Age: 238
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

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	http://google-gruyere.appspot.com/3826655807453863075471685123355512047 31/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	26087470|ZAP||author
Other Info	cookie:GRUYERE
URL	http://google-gruyere.appspot.com/3975875452656628180669215742395859497 62/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	26087470|ZAP||author
Other Info	cookie:GRUYERE
URL	http://google-gruyere.appspot.com/start
Method	GET
Attack	

Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/.
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/Applications
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/code/?resoources/dump.gtl
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/code/gruyere.py
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731

Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/gtl.py
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/opt/google/chrome
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/static/closed.gif
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/static/codeindex
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/static/codeindex.html
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/static/gruyere-40.png
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	http://google-gruyere.appspot.com/static/gruyere-badge.png
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID

URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
URL	https://google-gruyere.appspot.com/382665580745386307547168512335551204731/saveprofile?action=update&is_admin=True&uid=username
Method	GET
Attack	
Evidence	382665580745386307547168512335551204731
Other Info	cookie:GRUYERE_ID
Instances	19
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

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?

URL	pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/login?pw=ZAP&uid=ZAP
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
	http://google-gruyere.appspot.com/397587545265662818066921574239585949762

URL	/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://google-gruyere.appspot.com/397587545265662818066921574239585949762/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	48
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104