ZAP Scanning Report

Sites: https://googleads.g.doubleclick.net https://adservice.google.com.eg https://adservice.google.com https://play.google.com https://www.gstatic.com https://www.google.com https://remote-auth-gateway.discord.gg https://discord.com https://groups.google.com http://127.0.0.1:35769 https://www.google-analytics.com https://fonts.gstatic.com https://www.googletagmanager.com https://cdn.quilljs.com https://fonts.googleapis.com https://use.fontawesome.com http://127.0.0.1:2005

Generated on Thu, 11 Apr 2024 19:57:40

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	4
Medium	9
Low	13
Informational	13
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	2
Example High-Level Notification	High	1
PII Disclosure	High	1
SQL Injection	High	4
Absence of Anti-CSRF Tokens	Medium	7
CSP: Wildcard Directive	Medium	53
CSP: script-src unsafe-eval	Medium	11
CSP: style-src unsafe-inline	Medium	11
Content Security Policy (CSP) Header Not Set	Medium	16
Cross-Domain Misconfiguration	Medium	14
Example Medium-Level Notification	Medium	1

Session ID in URL Rewrite	Medium	51
Vulnerable JS Library	Medium	2
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1
CSP: Notices	Low	11
Cookie No HttpOnly Flag	Low	5
Cookie with SameSite Attribute None	Low	13
Cookie without SameSite Attribute	Low	7
Cross-Domain JavaScript Source File Inclusion	Low	16
Example Low-Level Notification	Low	1
HUD Tutorial Site Alert	Low	1
Private IP Disclosure	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	61
Strict-Transport-Security Header Not Set	Low	93
Timestamp Disclosure - Unix	Low	201
X-Content-Type-Options Header Missing	Low	58
Authentication Request Identified	Informational	1
Example Informational Alert Notification	Informational	1
GET for POST	Informational	11
HUD Tutorial Page Alert	Informational	1
Information Disclosure - Sensitive Information in URL	Informational	3
Information Disclosure - Suspicious Comments	Informational	186
Loosely Scoped Cookie	Informational	8
Modern Web Application	Informational	17
Re-examine Cache-control Directives	Informational	15
Retrieved from Cache	Informational	17
Session Management Response Identified	Informational	475
User Agent Fuzzer	Informational	624
User Controllable HTML Element Attribute (Potential XSS)	Informational	8

Alert Detail

High	**Cloud Metadata Potentially Exposed**
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	http://127.0.0.1:35769/latest/meta-data/

Method	GET
Parameter	
Attack	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
URL	http://127.0.0.1:35769/latest/meta-data/
Method	POST
Parameter	
Attack	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	2
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

High	**Example High-Level Notification**
Description	An example alert - this description will usually have more useful information in it!
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	60200

High	**PII Disclosure**
Description	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	585577383847788554
Other Info	Credit Card Type detected: Maestro Bank Identification Number: 585577 Brand: MAESTRO Category: Issuer:
Instances	1
Solution	Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.
Reference	
CWE Id	359
WASC Id	13
Plugin Id	10062

High	**SQL Injection**
Description	SQL injection may be possible.
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	content
Attack	console.log("Hello world");' AND '1'='1' --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [console.log("Hello world");' AND '1'='1' --] and [console.log("Hello world");' AND '1'='2' --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	language
Attack	javascript' OR '1'='1' --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [javascript' AND '1'='1' --] and [javascript' OR '1'='1' --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison Data was NOT returned for the original parameter. The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter
URL	http://127.0.0.1:2005/api/v2/piston/execute

Method	POST
Parameter	stdin
Attack	AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [AND 1=1 --] and [AND 1=2 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	version
Attack	/execute AND 1=1 --
Evidence	
Other Info	The page results were successfully manipulated using the boolean conditions [/execute AND 1=1 --] and [/execute AND 1=2 --] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter
Instances	4
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19

Plugin Id	40018
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://127.0.0.1:35769/Break
Method	GET
Parameter	
Attack	
Evidence	<form action="Break" method="post">
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: "number" "submit"].
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	
Attack	
Evidence	<form action="Enable" method="post">
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: "field1" "field2" "field3" "submit"].
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	

Attack	
Evidence	<form action="Show" method="post">
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: "field1" "field2" "field3" "field4" "submit"].
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	
Attack	
Evidence	<form class="tsf" action="/search" id="tsf" autocomplete="off" data-submitfalse="q" method="GET" name="f" role="search">
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: "client" "ei" "sca_esv" "sca_upv"].
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	
Attack	
Evidence	<form action="Break" method="post">
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: "number" "submit"].
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	
Attack	
Evidence	<form action="Enable" method="post">
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: "field1" "field2" "field3" "submit"].
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	
Attack	
Evidence	<form action="Show" method="post">

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: "field1" "field2" "field3" "field4" "submit"].
Instances	7
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	**CSP: Wildcard Directive**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://127.0.0.1:35769/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/ActiveScan

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/AjaxSpider

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/AlertNotifications

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/Alerts

Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Complete
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/HtmlReport
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/HudConfig
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Index
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the

	same as allowing anything.
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/ToggleScript

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/ToolConfig

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/Upgrade

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/Warning

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/WebSockets

Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://discord.com/api/v10/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	frame-ancestors 'none'; default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: form-action The directive(s): form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-MTQxLDE3Niw0Miw0LDE0MCwyMjksMTQxLDIyMw==' blob: https://cdn.discordapp.com/animations/ https://www.gstatic.com/recaptcha/ https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://js.braintreegateway.com https://assets.braintreegateway.com https://www.paypalobjects.com https://checkout.paypal.com https://c.paypal.com https://kit.cash.app; style-src 'self' 'unsafe-inline' https://cdn.discordapp.com https://*.hcaptcha.com https://hcaptcha.com https://kit.cash.app; img-src 'self' blob: data: https://*.discordapp.net https://*.discordapp.com https://*.discord.com https://i.scdn.co https://i.ytimg.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com https://*.youtube.com https://*.giphy.com https://static-cdn.jtvnw.net https://pbs.twimg.com https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com https://b.stats.paypal.com https://slc.stats.paypal.com https://hnd.stats.paypal.com https://api.cash.app; font-src 'self' https://fonts.gstatic.com https://cash-f.squarecdn.com; connect-src 'self' https://status.discordapp.com https://status.discord.com https://support.discordapp.com https://support.discord.com https://discordapp.com https://discord.com https://discord-attachments-uploads-prd.storage.googleapis.com https://cdn.discordapp.com https://media.discordapp.net https://images-ext-1.discordapp.net https://images-ext-2.discordapp.net https://router.discordapp.net wss://*.discord.gg https://best.discord.media https://latency.discord.media wss://*.discord.media wss://dealer.spotify.com https://api.spotify.com https://music.amazon.com/embed/oembed https://sentry.io https://api.twitch.tv https://api.stripe.com https://api.braintreegateway.com https://client-analytics.braintreegateway.com https://*.braintree-api.com https://www.googleapis.com https://*.algolianet.com https://*.hcaptcha.com https://hcaptcha.com https://*.algolia.net ws://127.0.0.1:* http://127.0.0.1:*; media-src 'self' blob: disclip: https://*.discordapp.net https://*.discord.com https://*.discordapp.com https://*.youtube.com https://streamable.com https://vid.me https://twitter.com

	https://oddshot.akamaized.net https://*.giphy.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com; frame-src https://discordapp.com/domain-migration discord: https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://hooks.stripe.com https://checkout.paypal.com https://c.paypal.com https://assets.braintreegateway.com https://checkoutshopper-live.adyen.com https://kit.cash.app https://player.twitch.tv https://clips.twitch.tv/embed https://player.vimeo.com https://www.youtube.com/embed/ https://www.tiktok.com/embed/ https://music.amazon.com/embed/ https://music.amazon.co.uk/embed/ https://music.amazon.de/embed/ https://music.amazon.co.jp/embed/ https://music.amazon.es/embed/ https://music.amazon.fr/embed/ https://music.amazon.it/embed/ https://music.amazon.com.au/embed/ https://music.amazon.in/embed/ https://music.amazon.ca/embed/ https://music.amazon.com.mx/embed/ https://music.amazon.com.br/embed/ https://www.youtube.com/s/player/ https://twitter.com/i/videos/ https://www.funimation.com/player/ https://www.redditmedia.com/mediaembed/ https://open.spotify.com/embed/ https://w.soundcloud.com/player/ https://audius.co/embed/ https://*.watchanimeattheoffice.com https://sessionshare.sp-int.playstation.com/embed/ https://localhost:* https://*.discordsays.com https://discordappcom.cloudflareaccess.com/; child-src 'self' blob: https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com; prefetch-src 'self' https://cdn.discordapp.com/assets/;
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-xt_reIfcxlHfqlaSDidG-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-vi8s1e9QU1ALSAVnrDXjkg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/compressiontest/gzip.html
Method	GET

Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-kR0ln8Gp4Y_Bdw2E8CN9sQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce--ZsGm-0PLSigRILZ_t2HBg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-duGTkUSXIuWD6jZNEs8uTQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the

	same as allowing anything.
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/History

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/PageAlerts

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/Scope

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/Show

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL http://127.0.0.1:35769/SiteAlerts

Method	POST

Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'none'; script-src 'self'; connect-src 'self'; child-src 'self'; img-src 'self' data:; font-src 'self' data:; style-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&nt=navigate&t=fi&st=4799&fid=1&zx=1712858085960&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-CHlTOTbV7LZjE3lNrLbWcQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	

Evidence	object-src 'none';base-uri 'self';script-src 'nonce-fJBHoJy2NnM2_zZM7IegKQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-o9vwyQm4n3OV2O6isKi2lA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-TimNoauzZPsrl5cYvLcPhg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&rt=wsrt.10,aft.1491,afti.1491,afts.877,frts.854,frvt.1491,hst.820,prt.888,sct.853&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-WSQN8zfMqmMgpISExY6f-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	53
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium **CSP: script-src unsafe-eval**

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-MTQxLDE3Niw0Miw0LDE0MCwyMjksMTQxLDIyMw==' blob: https://cdn.discordapp.com/animations/ https://www.gstatic.com/recaptcha/ https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://js.braintreegateway.com https://assets.braintreegateway.com https://www.paypalobjects.com https://checkout.paypal.com https://c.paypal.com https://kit.cash.app; style-src 'self' 'unsafe-inline' https://cdn.discordapp.com https://*.hcaptcha.com https://hcaptcha.com https://kit.cash.app; img-src 'self' blob: data: https://*.discordapp.net https://*.discordapp.com https://*.discord.com https://i.scdn.co https://i.ytimg.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com https://*.youtube.com https://*.giphy.com https://static-cdn.jtvnw.net https://pbs.twimg.com https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com https://b.stats.paypal.com https://slc.stats.paypal.com https://hnd.stats.paypal.com https://api.cash.app; font-src 'self' https://fonts.gstatic.com https://cash-f.squarecdn.com; connect-src 'self' https://status.discordapp.com https://status.discord.com https://support.discordapp.com https://support.discord.com https://discordapp.com https://discord.com https://discord-attachments-uploads-prd.storage.googleapis.com https://cdn.discordapp.com https://media.discordapp.net https://images-ext-1.discordapp.net https://images-ext-2.discordapp.net https://router.discordapp.net wss://*.discord.gg https://best.discord.media https://latency.discord.media wss://*.discord.media wss://dealer.spotify.com https://api.spotify.com https://music.amazon.com/embed/oembed https://sentry.io https://api.twitch.tv https://api.stripe.com https://api.braintreegateway.com https://client-analytics.braintreegateway.com https://*.braintree-api.com https://www.googleapis.com https://*.algolianet.com https://*.hcaptcha.com https://hcaptcha.com https://*.algolia.net ws://127.0.0.1:* http://127.0.0.1:*; media-src 'self' blob: disclip: https://*.discordapp.net https://*.discord.com https://*.discordapp.com https://*.youtube.com https://streamable.com https://vid.me https://twitter.com https://oddshot.akamaized.net https://*.giphy.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com; frame-src https://discordapp.com/domain-migration discord: https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://hooks.stripe.com https://checkout.paypal.com https://c.paypal.com https://assets.braintreegateway.com https://checkoutshopper-live.adyen.com https://kit.cash.app https://player.twitch.tv https://clips.twitch.tv/embed https://player.vimeo.com https://www.youtube.com/embed/ https://www.tiktok.com/embed/ https://music.amazon.com/embed/ https://music.amazon.co.uk/embed/ https://music.amazon.de/embed/ https://music.amazon.co.jp/embed/ https://music.amazon.es/embed/ https://music.amazon.fr/embed/ https://music.amazon.it/embed/ https://music.amazon.com.au/embed/ https://music.amazon.in/embed/ https://music.amazon.ca/embed/ https://music.amazon.com.mx/embed/ https://music.amazon.com.br/embed/ https://www.youtube.com/s/player/ https://twitter.com/i/videos/ https://www.funimation.com/player/ https://www.redditmedia.com/mediaembed/ https://open.spotify.com/embed/ https://w.soundcloud.com/player/ https://audius.co/embed/ https://*.watchanimeattheoffice.com https://sessionshare.sp-int.playstation.com/embed/ https://localhost:* https://*.discordsays.com https://discordappcom.cloudflareaccess.com/; child-src 'self' blob: https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com; prefetch-src 'self' https://cdn.discordapp.com/assets/;
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-xt_reIfcxlHfqlaSDidG-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/client_204?cs=1&opi=89978449

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-vi8s1e9QU1ALSAVnrDXjkg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-kR0In8Gp4Y_Bdw2E8CN9sQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce--ZsGm-0PLSigRILZ_t2HBg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-duGTkUSXIuWD6jZNEs8uTQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&nt=navigate&t=fi&st=4799&fid=1&zx=1712858085960&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	

Evidence	object-src 'none';base-uri 'self';script-src 'nonce-CHlTOTbV7LZjE3lNrLbWcQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-fJBHoJy2NnM2_zZM7IegKQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-o9vwyQm4n3OV2O6isKi2lA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-TimNoauzZPsrl5cYvLcPhg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&rt=wsrt.10,aft.1491,afti.1491,afts.877,frts.854,frvt.1491,hst.820,prt.888,sct.853&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-WSQN8zfMqmMgpISExY6f-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	script-src includes unsafe-eval.
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	Content-Security-Policy
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-MTQxLDE3Niw0Miw0LDE0MCwyMjksMTQxLDIyMw==' blob: https://cdn.discordapp.com/animations/ https://www.gstatic.com/recaptcha/ https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://js.braintreegateway.com https://assets.braintreegateway.com https://www.paypalobjects.com https://checkout.paypal.com https://c.paypal.com https://kit.cash.app; style-src 'self' 'unsafe-inline' https://cdn.discordapp.com https://*.hcaptcha.com https://hcaptcha.com https://kit.cash.app; img-src 'self' blob: data: https://*.discordapp.net https://*.discordapp.com https://*.discord.com https://i.scdn.co https://i.ytimg.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com https://*.youtube.com https://*.giphy.com https://static-cdn.jtvnw.net https://pbs.twimg.com https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com https://b.stats.paypal.com https://slc.stats.paypal.com https://hnd.stats.paypal.com https://api.cash.app; font-src 'self' https://fonts.gstatic.com https://cash-f.squarecdn.com; connect-src 'self' https://status.discordapp.com https://status.discord.com https://support.discordapp.com https://support.discord.com https://discordapp.com https://discord.com https://discord-attachments-uploads-prd.storage.googleapis.com https://cdn.discordapp.com https://media.discordapp.net https://images-ext-1.discordapp.net https://images-ext-2.discordapp.net https://router.discordapp.net wss://*.discord.gg https://best.discord.media https://latency.discord.media wss://*.discord.media wss://dealer.spotify.com https://api.spotify.com https://music.amazon.com/embed/oembed https://sentry.io https://api.twitch.tv https://api.stripe.com https://api.braintreegateway.com https://client-analytics.braintreegateway.com https://*.braintree-api.com https://www.googleapis.com https://*.algolianet.com https://*.hcaptcha.com https://hcaptcha.com https://*.algolia.net ws://127.0.0.1:* http://127.0.0.1:*; media-src 'self' blob: disclip: https://*.discordapp.net https://*.discord.com https://*.discordapp.com https://*.youtube.com https://streamable.com https://vid.me https://twitter.com https://oddshot.akamaized.net https://*.giphy.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com; frame-src https://discordapp.com/domain-migration discord: https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://hooks.stripe.com https://checkout.paypal.com https://c.paypal.com https://assets.braintreegateway.com https://checkoutshopper-live.adyen.com https://kit.cash.app https://player.twitch.tv https://clips.twitch.tv/embed https://player.vimeo.com https://www.youtube.com/embed/ https://www.tiktok.com/embed/ https://music.amazon.com/embed/ https://music.amazon.co.uk/embed/ https://music.amazon.de/embed/ https://music.amazon.co.jp/embed/ https://music.amazon.es/embed/ https://music.amazon.fr/embed/ https://music.amazon.it/embed/ https://music.amazon.com.au/embed/ https://music.amazon.in/embed/ https://music.amazon.ca/embed/ https://music.amazon.com.mx/embed/ https://music.amazon.com.br/embed/ https://www.youtube.com/s/player/ https://twitter.com/i/videos/ https://www.funimation.com/player/ https://www.redditmedia.com/mediaembed/ https://open.spotify.com/embed/ https://w.soundcloud.com/player/ https://audius.co/embed/ https://*.watchanimeattheoffice.com https://sessionshare.sp-int.playstation.com/embed/ https://localhost:* https://*.discordsays.com https://discordappcom.cloudflareaccess.com/; child-src 'self' blob: https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com; prefetch-src 'self' https://cdn.discordapp.com/assets/;
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-xt_reIfcxlHfqlaSDidG-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/client_204?cs=1&opi=89978449

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-vi8s1e9QU1ALSAVnrDXjkg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-kR0In8Gp4Y_Bdw2E8CN9sQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce--ZsGm-0PLSigRILZ_t2HBg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-duGTkUSXIuWD6jZNEs8uTQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&nt=navigate&t=fi&st=4799&fid=1&zx=1712858085960&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	

Evidence	object-src 'none';base-uri 'self';script-src 'nonce-CHlTOTbV7LZjE3lNrLbWcQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-fJBHoJy2NnM2_zZM7IegKQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-o9vwyQm4n3OV2O6isKi2lA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449

Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-TimNoauzZPsrl5cYvLcPhg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
URL	https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&rt=wsrt.10,aft.1491,afti.1491,afts.877,frts.854,frvt.1491,hst.820,prt.888,sct.853&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-WSQN8zfMqmMgpISExY6f-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	style-src includes unsafe-inline.
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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://127.0.0.1:2005/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	http://127.0.0.1:2005/@brikaasdev0096
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/challenges/create
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/create
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/challenges/44/python
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/challenges/choose_language/44
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests/24/asd

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/s/ROjOXc
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://googleads.g.doubleclick.net/adsid/google/si?gadsid=AORoGNSXIgFhYc0vN5WdURYIOShlj0O2LoU4dYoU110E3l3QJZm6ESEpiUej
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium **Cross-Domain Misconfiguration**

Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://127.0.0.1:2005/api/v1/piston/versions
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://127.0.0.1:2005/api/v2/piston/runtimes
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdn.quilljs.com/1.0.0/quill.snow.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://discord.com/cdn-cgi/challenge-platform/scripts/jsd/main.js
Method	GET
Parameter	
Attack	
Evidence	access-control-allow-origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.googleapis.com/css?family=Lato:100,300,400,700,900
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh50XSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh6UVSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh7USSwiPGQ.woff2
Method	GET
Parameter	
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.gstatic.com/s/lato/v24/S6uyw4BMUTPHjx4wXg.woff2
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.gstatic.com/s/notonaskharabicui/v4/9XU6lIJqkU_PWDHIY3lkVjo6pdPHBQyThjcnXyA.woff2
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://use.fontawesome.com/releases/v5.2.0/webfonts/fa-solid-900.woff2
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	14
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098
Medium	**Example Medium-Level Notification**
Description	An example alert - this description will usually have more useful information in it!
URL	http://127.0.0.1:35769/AlertNotifications

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	60200

Medium	**Session ID in URL Rewrite**
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712851965531&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712851967&sct=1&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_fv=1&_ss=1&tfd=2149
Method	POST
Parameter	sid
Attack	
Evidence	1712851967
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856522018&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_ss=1&tfd=1437
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856522018&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=21160&tfd=22604

Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856543884&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=page_view&tfd=5685
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856543884&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=user_engagement&_et=4685&tfd=8534
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856552333&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5153
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856552333&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=user_

	engagement&_et=23435&tfd=23573
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856575873&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fs%2FROjOXc&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5148
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856575873&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fs%2FROjOXc&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=10577&tfd=30172
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856606017&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fs%2FROjOXc&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5217
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856606017&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-

	us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fs%2FROjOXc&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=6414&tfd=42298
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856648285&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=page_view&tfd=5221
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856648285&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=user_engagement&_et=6025&tfd=6170
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856654407&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2023
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856656403&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3272
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856659658&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5333
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856659658&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=13848&tfd=22862
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856682466&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5193
Method	POST
Parameter	sid

Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856682466&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=6412&tfd=47686
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856730131&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2Fchoose_language%2F44&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Coding%20Challenges%20%7C%20EMKC&_s=1&tfd=1693
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856731650&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2F44%2Fpython&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2Fchoose_language%2F44&dt=Easy%20Challenge%3A%20test%20%7C%20EMKC&en=page_view&tfd=5150
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856731650&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2F44%2Fpython&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2Fchoose_language%2F44&dt=Easy%20Challenge%3A%20test%20%7C

	%20EMKC&en=user_engagement&_et=12655&tfd=12811
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856744442&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2F44%2Fpython&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3904
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856748157&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F%40brikaasdev0096&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=brikaasdev0096%20-%20EMKC%20Member&_s=1&tfd=4311
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856752348&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F%40brikaasdev0096&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=3955
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856756200&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2

	F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3377
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856759166&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3838
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856762695&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5257
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856762695&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=8673&tfd=8927
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856771496&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2264
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856773723&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=4222
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856777863&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1532
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856779225&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2151
Method	POST
Parameter	sid
Attack	
Evidence	1712856522

Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856781287&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fupdate%2F24&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=5000
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856786235&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests%2Fupdate%2F24&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1955
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856788125&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5188
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856788125&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=5963&tfd=6157
Method	POST

Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856794241&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=1667
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856795767&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=page_view&tfd=5183
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856795767&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=user_engagement&_et=33871&tfd=34058
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856829764&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=page_view&tfd=5510

Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856829764&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=user_engagement&_et=8803&tfd=33270
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856885583&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests%2F24%2Fasd&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=2213
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856887735&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=3345
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856926269&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2

	F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1748
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856927983&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=873
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856928845&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5497
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856928845&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=44551&tfd=387552
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857324978&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%

	3A%2F%2F127.0.0.1%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Coding%20Challenges%20%7C%20EMKC&en=page_view&tfd=5220
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857324978&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Coding%20Challenges%20%7C%20EMKC&en=user_engagement&_et=8257&tfd=8471
Method	POST
Parameter	sid
Attack	
Evidence	1712856522
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857829595&gcd=13l3l3l3l1&npa=0&dma=0&cid=1018073132.1712857831&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712857830&sct=1&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_fv=1&_nsi=1&_ss=1&tfd=1566
Method	POST
Parameter	sid
Attack	
Evidence	1712857830
Other Info	
Instances	51
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	200
WASC Id	13
Plugin Id	3
Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 3.0.0 is vulnerable.
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET

Parameter	
Attack	
Evidence	* Bootstrap v4.1.3
Other Info	CVE-2019-8331
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	
Attack	
Evidence	jquery-3.0.0.min.js
Other Info	CVE-2020-11023 CVE-2020-11022 CVE-2019-11358
Instances	2
Solution	Please upgrade to the latest version of jquery.
Reference	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

Low	**Big Redirect Detected (Potential Sensitive Information Leak)**
Description	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	https://discord.com/api/v10/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	
Attack	
Evidence	
Other Info	Location header URI length: 170 [https://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email]. Predicted response size: 470. Response Body Length: 571.
Instances	1
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201
WASC Id	13

Plugin Id	10044
Low	**CSP: Notices**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-MTQxLDE3Niw0Miw0LDE0MCwyMjksMTQxLDIyMw==' blob: https://cdn.discordapp.com/animations/ https://www.gstatic.com/recaptcha/ https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://js.braintreegateway.com https://assets.braintreegateway.com https://www.paypalobjects.com https://checkout.paypal.com https://c.paypal.com https://kit.cash.app; style-src 'self' 'unsafe-inline' https://cdn.discordapp.com https://*.hcaptcha.com https://hcaptcha.com https://kit.cash.app; img-src 'self' blob: data: https://*.discordapp.net https://*.discordapp.com https://*.discord.com https://i.scdn.co https://i.ytimg.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com https://*.youtube.com https://*.giphy.com https://static-cdn.jtvnw.net https://pbs.twimg.com https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com https://b.stats.paypal.com https://slc.stats.paypal.com https://hnd.stats.paypal.com https://api.cash.app; font-src 'self' https://fonts.gstatic.com https://cash-f.squarecdn.com; connect-src 'self' https://status.discordapp.com https://status.discord.com https://support.discordapp.com https://support.discord.com https://discordapp.com https://discord.com https://discord-attachments-uploads-prd.storage.googleapis.com https://cdn.discordapp.com https://media.discordapp.net https://images-ext-1.discordapp.net https://images-ext-2.discordapp.net https://router.discordapp.net wss://*.discord.gg https://best.discord.media https://latency.discord.media wss://*.discord.media wss://dealer.spotify.com https://api.spotify.com https://music.amazon.com/embed/oembed https://sentry.io https://api.twitch.tv https://api.stripe.com https://api.braintreegateway.com https://client-analytics.braintreegateway.com https://*.braintree-api.com https://www.googleapis.com https://*.algolianet.com https://*.hcaptcha.com https://hcaptcha.com https://*.algolia.net ws://127.0.0.1:* http://127.0.0.1:*; media-src 'self' blob: disclip: https://*.discordapp.net https://*.discord.com https://*.discordapp.com https://*.youtube.com https://streamable.com https://vid.me https://twitter.com https://oddshot.akamaized.net https://*.giphy.com https://i.imgur.com https://media.tenor.co https://media.tenor.com https://c.tenor.com; frame-src https://discordapp.com/domain-migration discord: https://www.google.com/recaptcha/ https://recaptcha.net/recaptcha/ https://*.hcaptcha.com https://hcaptcha.com https://js.stripe.com https://hooks.stripe.com https://checkout.paypal.com https://c.paypal.com https://assets.braintreegateway.com https://checkoutshopper-live.adyen.com https://kit.cash.app https://player.twitch.tv https://clips.twitch.tv/embed https://player.vimeo.com https://www.youtube.com/embed/ https://www.tiktok.com/embed/ https://music.amazon.com/embed/ https://music.amazon.co.uk/embed/ https://music.amazon.de/embed/ https://music.amazon.co.jp/embed/ https://music.amazon.es/embed/ https://music.amazon.fr/embed/ https://music.amazon.it/embed/ https://music.amazon.com.au/embed/ https://music.amazon.in/embed/ https://music.amazon.ca/embed/ https://music.amazon.com.mx/embed/ https://music.amazon.com.br/embed/ https://www.youtube.com/s/player/ https://twitter.com/i/videos/ https://www.funimation.com/player/ https://www.redditmedia.com/mediaembed/ https://open.spotify.com/embed/ https://

	w.soundcloud.com/player/ https://audius.co/embed/ https://*.watchanimeattheoffice.com https://sessionshare.sp-int.playstation.com/embed/ https://localhost:* https://*.discordsays.com https://discordappcom.cloudflareaccess.com/; child-src 'self' blob: https://assets.braintreegateway.com https://checkout.paypal.com https://c.paypal.com; prefetch-src 'self' https://cdn.discordapp.com/assets/;
Other Info	Warnings: The prefetch-src directive has been deprecated
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-xt_reIfcxlHfqlaSDidG-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-vi8s1e9QU1ALSAVnrDXjkg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-kR0ln8Gp4Y_Bdw2E8CN9sQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce--ZsGm-0PLSigRILZ_t2HBg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-duGTkUSXIuWD6jZNEs8uTQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/fff
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&nt=navigate&t=fi&st=4799&fid=1&zx=1712858085960&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-CHITOTbV7LZjE3lNrLbWcQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-fJBHoJy2NnM2_zZM7IegKQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,

	1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-o9vwyQm4n3OV2O6isKi2lA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-TimNoauzZPsrl5cYvLcPhg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&rt=wsrt.10,aft.1491,afti.1491,afts.877,frts.854,frvt.1491,hst.820,prt.888,sct.853&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&opi=89978449
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-WSQN8zfMqmMgpISExY6f-A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15

Plugin Id	10055
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	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	1P_JAR

Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
Instances	5
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 with SameSite Attribute None**

Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://adservice.google.com/adsid/google/si?gadsid=AORoGNRfzEOEOU6HVESnimbmzwWbmes6qJ1Dq5ge5O5Rn1CY2_x6WyhEB5AW
Method	GET
Parameter	ANID
Attack	
Evidence	Set-Cookie: ANID
Other Info	
URL	https://discord.com/api/v10/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	__cfruid
Attack	
Evidence	Set-Cookie: __cfruid
Other Info	
URL	https://discord.com/api/v10/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	_cfuvid
Attack	
Evidence	Set-Cookie: _cfuvid
Other Info	
URL	https://groups.google.com/group/zaproxy-hud
Method	GET

Parameter	NID
Attack	
Evidence	Set-Cookie: NID
Other Info	
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET
Parameter	NID
Attack	
Evidence	Set-Cookie: NID
Other Info	
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	

Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	1P_JAR
Attack	
Evidence	Set-Cookie: 1P_JAR
Other Info	
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	NID
Attack	
Evidence	Set-Cookie: NID
Other Info	
URL	https://discord.com/cdn-cgi/challenge-platform/h/b/jsd/r/872cb0975e860fd6
Method	POST
Parameter	cf_clearance
Attack	
Evidence	Set-Cookie: cf_clearance
Other Info	
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Parameter	NID
Attack	
Evidence	Set-Cookie: NID
Other Info	
Instances	13
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	**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://127.0.0.1:2005/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
URL	http://127.0.0.1:2005/auth/discord_cb?code=NUnqDUNeHxMt9LjAEYdpmfxHDh4buM
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	engineerman.sid

Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
URL	http://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	set-cookie: engineerman.sid
Other Info	
Instances	7
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://127.0.0.1:2005/
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/@brikaasdev0096
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/admin
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	

URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/admin/challenges/create
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/admin/contests/create
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	

Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/challenges/44/python
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/challenges/choose_language/44
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/s/ROjOXc
Method	GET
Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET

Parameter	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Attack	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-28939284-9"></script>
Other Info	
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWlMsg
Attack	
Evidence	<script async="" nonce="duGTkUSXIuWD6jZNEs8uTQ" src="https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWlMsg"></script>
Other Info	
Instances	16
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Example Low-Level Notification**
Description	An example alert - this description will usually have more useful information in it!
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	60200

Low	**HUD Tutorial Site Alert**
Description	This alert is associated with a JavaScript file so you would only see Page Alerts for it if you manually opened it in your browser. However, you will see any alerts related to it in the Site Alert tools. You can see the request and response associated with the alert by clicking on the URL above. In this case, the key you need is in the response body.

URL	http://127.0.0.1:35769/SiteAlerts.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	60200

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://discord.com/assets/19878.38577e57248a8460bd91.js
Method	GET
Parameter	
Attack	
Evidence	10.8.2.2
Other Info	10.8.2.2
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/ PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Parameter	
Attack	

Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712851965531&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712851967&sct=1&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_fv=1&_ss=1&tfd=2149
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856522018&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_ss=1&tfd=1437
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856522018&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=21160&tfd=22604
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856543884&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=page_view&tfd=5685
Method	POST
Parameter	

Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856543884&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=user_engagement&_et=4685&tfd=8534
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856552333&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5153
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856552333&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=23435&tfd=23573
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856575873&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fs%2FROjOXc&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5148
Method	POST

Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856575873&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fs%2FROjOXc&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=10577&tfd=30172
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856606017&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fs%2FROjOXc&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5217
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856606017&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fs%2FROjOXc&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=6414&tfd=42298
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856648285&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=page_view&tfd=5221

Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856648285&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=user_engagement&_et=6025&tfd=6170
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856654407&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2023
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856656403&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3272
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856659658&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3

	A2005%2Fadmin%2Fchallenges&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5333
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856659658&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=13848&tfd=22862
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856682466&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5193
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856682466&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=6412&tfd=47686
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856730131&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2Fchoose_language%2F44&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Coding%20Challenges%20%7C%20EMKC&_s=1&tfd=1693
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856731650&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2F44%2Fpython&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2Fchoose_language%2F44&dt=Easy%20Challenge%3A%20test%20%7C%20EMKC&en=page_view&tfd=5150
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856731650&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2F44%2Fpython&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2Fchoose_language%2F44&dt=Easy%20Challenge%3A%20test%20%7C%20EMKC&en=user_engagement&_et=12655&tfd=12811
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856744442&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2F44%2Fpython&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3904
Method	POST
Parameter	

Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856748157&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F%40brikaasdev0096&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=brikaasdev0096%20-%20EMKC%20Member&_s=1&tfd=4311
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856752348&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F%40brikaasdev0096&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=3955
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856756200&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3377
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856759166&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3838
Method	POST

Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856762695&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5257
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856762695&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=8673&tfd=8927
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856771496&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2264
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856773723&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests

	&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=4222
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856777863&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1532
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856779225&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2151
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856781287&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fupdate%2F24&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=5000
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856786235&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-

	us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests%2Fupdate%2F24&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1955
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856788125&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5188
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856788125&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=5963&tfd=6157
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856794241&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=1667
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856795767&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=page_view&tfd=5183
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856795767&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=user_engagement&_et=33871&tfd=34058
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856829764&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=page_view&tfd=5510
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856829764&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=user_engagement&_et=8803&tfd=33270
Method	POST
Parameter	
Attack	

Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856885583&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests%2F24%2Fasd&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=2213
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856887735&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=3345
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856926269&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1748
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856927983&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=873
Method	POST
Parameter	
Attack	

Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856928845&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5497
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856928845&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=44551&tfd=387552
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857324978&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Coding%20Challenges%20%7C%20EMKC&en=page_view&tfd=5220
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857324978&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Coding%20Challenges%20%7C%20EMKC&en=user_engagement&_et=8257&tfd=8471
Method	POST
Parameter	

Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857829595&gcd=13l3l3l3l1&npa=0&dma=0&cid=1018073132.1712857831&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712857830&sct=1&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_fv=1&_nsi=1&_ss=1&tfd=1566
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1004712329&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&ul=en-us&de=UTF-8&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1027411131&gjid=1194625269&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=401505989
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1407520491&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1687499031&gjid=1594761401&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=603804996
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=229984120&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=YADAAUABAAAAACAAI~&jid=1269294845&gjid=425644706&cid=1018073132.1712857831&tid=UA-28939284-9&_gid=786141185.1712857832&_r=1&gtm=457e44a0h2za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=843975175
Method	POST

Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=262784116&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=YEBAAUABAAAAACAAI~&jid=1875684015&gjid=625783077&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=1134744223
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=425861281&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1798274475&gjid=1641218229&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=916569866
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=456473969&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&ul=en-us&de=UTF-8&dt=Coding%20Challenges%20%7C%20EMKC&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=448930181&gjid=2064181401&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=291423297
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=570666341&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=290841553&gjid=577310014&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=1769927305

Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=637183378&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1004041412&gjid=1040001354&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=1188413680
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=865757751&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=635852305&gjid=246010562&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=1981113649
Method	POST
Parameter	
Attack	
Evidence	Golfe2
Other Info	
Instances	61
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	200
WASC Id	13
Plugin Id	10036

Low **Strict-Transport-Security Header Not Set**

Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

URL	https://adservice.google.com.eg/adsid/google/si?gadsid=AORoGNRve03b4_YvmWBm8hEzPoeATFkC3C4c9aqofxhByFj8ZcvYyH7qpbz1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://adservice.google.com.eg/adsid/google/ui?gadsid=AORoGNSdmJPoP4qJc_fa4urv3NcKqb2x-3AsGQNw4YZb6dSpcyk7SKVBhg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://adservice.google.com/adsid/google/si?gadsid=AORoGNRfzEOEOU6HVESnimbmzwWbmes6qJ1Dq5ge5O5Rn1CY2_x6WyhEB5AW
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://adservice.google.com/adsid/google/ui
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://cdn.quilljs.com/1.0.0/quill.snow.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh50XSwiPGQ.woff2
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh6UVSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh7USSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/lato/v24/S6uyw4BMUTPHjx4wXg.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/notonaskharabicui/v4/9XU6lIJqkU_PWDHIY3lkVjo6pdPHBQyThjcnXyA.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://googleads.g.doubleclick.net/adsid/google/si?gadsid=AORoGNSXIgFhYc0vN5WdURYIOShIj0O2LoU4dYoU110E3l3QJZm6ESEpiUej
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNSwC_S1VHNY1IZxEMvbc9mtgSQYPkASMHogqr290V8ifqoKWtwJzWug
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://use.fontawesome.com/releases/v5.2.0/css/all.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://use.fontawesome.com/releases/v5.2.0/webfonts/fa-solid-900.woff2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-

	FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAME6AcAAAAAAAAA AAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAAB AAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/ rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=kMFpHd,sy8q,bm51tf?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgC AAQAEAAVgGyECAAQQDAABCCAH7- FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAME6AcAAAAAAAAA AAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAAB AAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/ rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ m=sy3tf,sy483,w4UyN,syx8,syx9,EbPKJf,sy4nm,sy6x3,J9Q59e,sy4nn,a6Sgfb,Tia57b,KpRAue,s y14u,NyeqM,sy2nk,sy2nl,O9SqHb?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgC AAQAEAAVgGyECAAQQDAABCCAH7- FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAME6AcAAAAAAAAA AAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAAB AAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/ rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=syfa,syfb,aLUfP?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgC AAQAEAAVgGyECAAQQDAABCCAH7- FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAME6AcAAAAAAAAA AAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAAB AAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/ rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv ,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr, sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syx g,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy 1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/

	excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQ

	Od;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GEIbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tlj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/js/md=3/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/xjs/_/ss/k=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAhAACAcIAAsAEAAPjgEABAAAAQAAACBAEAAIAAQQDAAACAAAAABAAAHIAAAACEAUCAAAQIIAmBDAQAIAITDJAKAAAw_AgAAQAIAAAAEBAAgIAABwEMUCAgGgAAiEAAEAQCAA0IAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAEAAAAAAAAAAAAAAAAAAACA/d=1/ed=1/rs=ACT90oE-MPIqTKuW95aUgrdlMfX6GEt0qQ/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/og/_/ss/k=og.asy.DzP_dblOEpw.R.F4.O/m=ll_tdm,adc,ll_fw/excm=/d=1/ed=1/ct=zgms/rs=AA2YrTsmw3C5zSuPckfjJ3sSxBCz1yduSA
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712851965531&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712851967&sct=1&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_fv=1&_ss=1&tfd=2149
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856522018&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_ss=1&tfd=1437
Method	POST

Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856522018&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=21160&tfd=22604
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856543884&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=page_view&tfd=5685
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856543884&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=user_engagement&_et=4685&tfd=8534
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856552333&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5153

Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856552333&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=23435&tfd=23573
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856575873&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fs%2FROjOXc&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5148
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856575873&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fs%2FROjOXc&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fsnippets&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=10577&tfd=30172
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856606017&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%

	3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fs%2FROjOXc&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5217
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856606017&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fs%2FROjOXc&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=6414&tfd=42298
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856648285&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=page_view&tfd=5221
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856648285&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Weekly%20Contests%20%7C%20EMKC&en=user_engagement&_et=6025&tfd=6170
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856654407&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-

	us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2023
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856656403&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3272
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856659658&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5333
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856659658&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=13848&tfd=22862
Method	POST
Parameter	
Attack	
Evidence	
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856682466&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5193
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856682466&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=6412&tfd=47686
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856730131&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2Fchoose_language%2F44&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fchallenges&dt=Coding%20Challenges%20%7C%20EMKC&_s=1&tfd=1693
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856731650&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2F44%2Fpython&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2Fchoose_language%2F44&dt=Easy%20Challenge%3A%20test%20%7C%20EMKC&en=page_view&tfd=5150
Method	POST
Parameter	

Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856731650&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges%2F44%2Fpython&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2Fchoose_language%2F44&dt=Easy%20Challenge%3A%20test%20%7C%20EMKC&en=user_engagement&_et=12655&tfd=12811
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856744442&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fchallenges%2F44%2Fpython&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3904
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856748157&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F%40brikaasdev0096&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=brikaasdev0096%20-%20EMKC%20Member&_s=1&tfd=4311
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856752348&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2F%40brikaasdev0096&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=3955
Method	POST

Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856756200&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3377
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856759166&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=3838
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856762695&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5257
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856762695&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fcreate&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=user_engage

ment&_et=8673&tfd=8927

Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856771496&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests%2Fcreate&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2264
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856773723&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=4222
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856777863&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1532
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856779225&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2

	F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=2151
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856781287&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests%2Fupdate%2F24&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=5000
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856786235&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests%2Fupdate%2F24&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1955
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856788125&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5188
Method	POST
Parameter	
Attack	
Evidence	
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856788125&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=5963&tfd=6157
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856794241&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fadmin%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=1667
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856795767&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=page_view&tfd=5183
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856795767&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=user_engagement&_et=33871&tfd=34058
Method	POST
Parameter	
Attack	

Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856829764&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=page_view&tfd=5510
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856829764&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&en=user_engagement&_et=8803&tfd=33270
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856885583&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests%2F24%2Fasd&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=2213
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856887735&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests&dr=https%3A%2F%2F127.0.0.1%3A2005%2Fcontests&dt=Weekly%20Contests%20%7C%20EMKC&_s=1&tfd=3345
Method	POST
Parameter	

Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856926269&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&_s=1&tfd=1748
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856927983&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=873
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856928845&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&tfd=5497
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712856928845&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=user_engagement&_et=44551&tfd=387552
Method	POST
Parameter	

Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857324978&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Coding%20Challenges%20%7C%20EMKC&en=page_view&tfd=5220
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857324978&gcd=13l3l3l3l1&npa=0&dma=0&cid=1475577130.1712851967&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=2&sid=1712856522&sct=2&seg=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&dr=https%3A%2F%2F127.0.0.1%3A2005%2F&dt=Coding%20Challenges%20%7C%20EMKC&en=user_engagement&_et=8257&tfd=8471
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-N33Q40M7WG&gtm=45je4480v9112419235za200&_p=1712857829595&gcd=13l3l3l3l1&npa=0&dma=0&cid=1018073132.1712857831&ul=en-us&sr=2048x1152&pscdl=noapi&_eu=AAAI&_s=1&sid=1712857830&sct=1&seg=0&dl=https%3A%2F%2F127.0.0.1%2F&dt=Engineer%20Man%20Knowledge%20Center&en=page_view&_fv=1&_nsi=1&_ss=1&tfd=1566
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1004712329&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2Fcontests%2F24%2Fasd&ul=en-us&de=UTF-8&dt=Coding%20Contest%3A%20asd%20%7C%20EMKC&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1027411131&gjid=1194625269&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=401505989
Method	POST

Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1407520491&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1687499031&gjid=1594761401&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=603804996
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=229984120&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=YADAAUABAAAAACAAI~&jid=1269294845&gjid=425644706&cid=1018073132.1712857831&tid=UA-28939284-9&_gid=786141185.1712857832&_r=1&gtm=457e44a0h2za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=843975175
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=262784116&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=YEBAAUABAAAAACAAI~&jid=1875684015&gjid=625783077&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=1134744223
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=425861281&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1798274475&gjid=1641218229&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=916569866

Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=456473969&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2Fchallenges&ul=en-us&de=UTF-8&dt=Coding%20Challenges%20%7C%20EMKC&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=448930181&gjid=2064181401&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l3l1&dma=0&jsscut=1&z=291423297
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=570666341&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2Fadmin%2Fchallenges&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=290841553&gjid=577310014&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l3l1&dma=0&jsscut=1&z=1769927305
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=637183378&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=1004041412&gjid=1040001354&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967&_r=1&gtm=457e4480za200&gcd=13l3l3l3l3l1&dma=0&jsscut=1&z=1188413680
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google-analytics.com/j/collect?v=1&_v=j101&a=865757751&t=pageview&_s=1&dl=https%3A%2F%2F127.0.0.1%2F&ul=en-us&de=UTF-8&dt=Engineer%20Man%20Knowledge%20Center&sd=24-bit&sr=2048x1152&vp=1288x701&je=0&_u=QACAAUABAAAAACAAI~&jid=635852305&gjid=246010562&cid=1475577130.1712851967&tid=UA-28939284-9&_gid=629965141.1712851967

	&_r=1&gtm=457e4480za200&gcd=13l3l3l3l1&dma=0&jsscut=1&z=1981113649
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&nt=navigate&t=fi&st=4799&fid=1&zx=1712858085960&opi=89978449
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,

	578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&rt=wsrt.10,aft.1491,afti.1491,afts.877,frts.854,frvt.1491,hst.820,prt.888,sct.853&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&opi=89978449
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
Instances	93
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://discord.com/api/v10/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET

Parameter	Set-Cookie
Attack	
Evidence	1712856472
Other Info	1712856472, which evaluates to: 2024-04-11 19:27:52
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1398007839
Other Info	1398007839, which evaluates to: 2014-04-20 17:30:39
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1398673921
Other Info	1398673921, which evaluates to: 2014-04-28 10:32:01
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1400254877
Other Info	1400254877, which evaluates to: 2014-05-16 18:41:17
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1443856828
Other Info	1443856828, which evaluates to: 2015-10-03 09:20:28
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1454135605
Other Info	1454135605, which evaluates to: 2016-01-30 08:33:25

URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1459591700
Other Info	1459591700, which evaluates to: 2016-04-02 12:08:20
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1495876933
Other Info	1495876933, which evaluates to: 2017-05-27 11:22:13
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1503364285
Other Info	1503364285, which evaluates to: 2017-08-22 03:11:25
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1531667641
Other Info	1531667641, which evaluates to: 2018-07-15 17:14:01
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1532280548
Other Info	1532280548, which evaluates to: 2018-07-22 19:29:08
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	

Evidence	1549543958
Other Info	1549543958, which evaluates to: 2019-02-07 14:52:38
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1567199723
Other Info	1567199723, which evaluates to: 2019-08-30 23:15:23
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1580712211
Other Info	1580712211, which evaluates to: 2020-02-03 08:43:31
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1609782151
Other Info	1609782151, which evaluates to: 2021-01-04 19:42:31
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1617749743
Other Info	1617749743, which evaluates to: 2021-04-07 00:55:43
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1617769333
Other Info	1617769333, which evaluates to: 2021-04-07 06:22:13
URL	https://discord.com/api/v9/experiments
Method	GET

Parameter	
Attack	
Evidence	1631741096
Other Info	1631741096, which evaluates to: 2021-09-15 23:24:56
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1680860120
Other Info	1680860120, which evaluates to: 2023-04-07 11:35:20
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1690640008
Other Info	1690640008, which evaluates to: 2023-07-29 17:13:28
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1779058233
Other Info	1779058233, which evaluates to: 2026-05-18 01:50:33
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1788933951
Other Info	1788933951, which evaluates to: 2026-09-09 09:05:51
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1794801891
Other Info	1794801891, which evaluates to: 2026-11-16 06:04:51

URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1794874227
Other Info	1794874227, which evaluates to: 2026-11-17 02:10:27
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1814483290
Other Info	1814483290, which evaluates to: 2027-07-02 02:08:10
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1834860859
Other Info	1834860859, which evaluates to: 2028-02-22 21:34:19
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1851544364
Other Info	1851544364, which evaluates to: 2028-09-03 00:52:44
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1859132618
Other Info	1859132618, which evaluates to: 2028-11-29 19:43:38
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	

Evidence	1869634267
Other Info	1869634267, which evaluates to: 2029-03-31 08:51:07
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1881851350
Other Info	1881851350, which evaluates to: 2029-08-19 19:29:10
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1884426471
Other Info	1884426471, which evaluates to: 2029-09-18 14:47:51
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1894288113
Other Info	1894288113, which evaluates to: 2030-01-10 17:08:33
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1913882179
Other Info	1913882179, which evaluates to: 2030-08-25 12:56:19
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	
Attack	
Evidence	1944696695
Other Info	1944696695, which evaluates to: 2031-08-17 04:31:35
URL	https://discord.com/api/v9/experiments
Method	GET

Parameter	
Attack	
Evidence	1973330780
Other Info	1973330780, which evaluates to: 2032-07-13 14:26:20
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1398007839
Other Info	1398007839, which evaluates to: 2014-04-20 17:30:39
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1398673921
Other Info	1398673921, which evaluates to: 2014-04-28 10:32:01
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1400254877
Other Info	1400254877, which evaluates to: 2014-05-16 18:41:17
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1405831955
Other Info	1405831955, which evaluates to: 2014-07-20 06:52:35
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1412337990
Other Info	1412337990, which evaluates to: 2014-10-03 14:06:30

URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1431352750
Other Info	1431352750, which evaluates to: 2015-05-11 15:59:10
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1443856828
Other Info	1443856828, which evaluates to: 2015-10-03 09:20:28
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1443876045
Other Info	1443876045, which evaluates to: 2015-10-03 14:40:45
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1454135605
Other Info	1454135605, which evaluates to: 2016-01-30 08:33:25
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1459591700
Other Info	1459591700, which evaluates to: 2016-04-02 12:08:20
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	

Evidence	1485389700
Other Info	1485389700, which evaluates to: 2017-01-26 02:15:00
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1487316075
Other Info	1487316075, which evaluates to: 2017-02-17 09:21:15
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1489979462
Other Info	1489979462, which evaluates to: 2017-03-20 05:11:02
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1495876933
Other Info	1495876933, which evaluates to: 2017-05-27 11:22:13
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1496165720
Other Info	1496165720, which evaluates to: 2017-05-30 19:35:20
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1503364285
Other Info	1503364285, which evaluates to: 2017-08-22 03:11:25
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET

Parameter	
Attack	
Evidence	1504498621
Other Info	1504498621, which evaluates to: 2017-09-04 06:17:01
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1512150978
Other Info	1512150978, which evaluates to: 2017-12-01 19:56:18
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1531667641
Other Info	1531667641, which evaluates to: 2018-07-15 17:14:01
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1532280548
Other Info	1532280548, which evaluates to: 2018-07-22 19:29:08
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1549543958
Other Info	1549543958, which evaluates to: 2019-02-07 14:52:38
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1567199723
Other Info	1567199723, which evaluates to: 2019-08-30 23:15:23

URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1570379293
Other Info	1570379293, which evaluates to: 2019-10-06 18:28:13
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1580712211
Other Info	1580712211, which evaluates to: 2020-02-03 08:43:31
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1604612045
Other Info	1604612045, which evaluates to: 2020-11-05 23:34:05
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1609782151
Other Info	1609782151, which evaluates to: 2021-01-04 19:42:31
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1617749743
Other Info	1617749743, which evaluates to: 2021-04-07 00:55:43
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	

Evidence	1631741096
Other Info	1631741096, which evaluates to: 2021-09-15 23:24:56
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1640064366
Other Info	1640064366, which evaluates to: 2021-12-21 07:26:06
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1643537656
Other Info	1643537656, which evaluates to: 2022-01-30 12:14:16
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1669115628
Other Info	1669115628, which evaluates to: 2022-11-22 13:13:48
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1680860120
Other Info	1680860120, which evaluates to: 2023-04-07 11:35:20
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1689901851
Other Info	1689901851, which evaluates to: 2023-07-21 04:10:51
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET

Parameter	
Attack	
Evidence	1690640008
Other Info	1690640008, which evaluates to: 2023-07-29 17:13:28
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1727857487
Other Info	1727857487, which evaluates to: 2024-10-02 11:24:47
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1765194502
Other Info	1765194502, which evaluates to: 2025-12-08 13:48:22
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1779058233
Other Info	1779058233, which evaluates to: 2026-05-18 01:50:33
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1788933951
Other Info	1788933951, which evaluates to: 2026-09-09 09:05:51
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1794801891
Other Info	1794801891, which evaluates to: 2026-11-16 06:04:51

URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1794874227
Other Info	1794874227, which evaluates to: 2026-11-17 02:10:27
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1804122827
Other Info	1804122827, which evaluates to: 2027-03-04 03:13:47
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1814483290
Other Info	1814483290, which evaluates to: 2027-07-02 02:08:10
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1834860859
Other Info	1834860859, which evaluates to: 2028-02-22 21:34:19
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1859132618
Other Info	1859132618, which evaluates to: 2028-11-29 19:43:38
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	

Evidence	1865413295
Other Info	1865413295, which evaluates to: 2029-02-10 12:21:35
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1869634267
Other Info	1869634267, which evaluates to: 2029-03-31 08:51:07
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1884426471
Other Info	1884426471, which evaluates to: 2029-09-18 14:47:51
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1894288113
Other Info	1894288113, which evaluates to: 2030-01-10 17:08:33
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1913882179
Other Info	1913882179, which evaluates to: 2030-08-25 12:56:19
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1926000171
Other Info	1926000171, which evaluates to: 2031-01-12 18:02:51
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET

Parameter	
Attack	
Evidence	1944696695
Other Info	1944696695, which evaluates to: 2031-08-17 04:31:35
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1973330780
Other Info	1973330780, which evaluates to: 2032-07-13 14:26:20
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1979035979
Other Info	1979035979, which evaluates to: 2032-09-17 15:12:59
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1982804121
Other Info	1982804121, which evaluates to: 2032-10-31 04:55:21
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	1990672009
Other Info	1990672009, which evaluates to: 2033-01-30 06:26:49
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	2001176293
Other Info	2001176293, which evaluates to: 2033-05-31 21:18:13

URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	2009396848
Other Info	2009396848, which evaluates to: 2033-09-04 00:47:28
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	
Attack	
Evidence	2014775304
Other Info	2014775304, which evaluates to: 2033-11-05 05:48:24
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1426881987
Other Info	1426881987, which evaluates to: 2015-03-20 22:06:27
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1431655765
Other Info	1431655765, which evaluates to: 2015-05-15 04:09:25
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1432725776
Other Info	1432725776, which evaluates to: 2015-05-27 13:22:56
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	

Evidence	1433087999
Other Info	1433087999, which evaluates to: 2015-05-31 17:59:59
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1467031594
Other Info	1467031594, which evaluates to: 2016-06-27 14:46:34
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1495990901
Other Info	1495990901, which evaluates to: 2017-05-28 19:01:41
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1501505948
Other Info	1501505948, which evaluates to: 2017-07-31 14:59:08
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-26 00:36:33
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 07:37:29
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET

Parameter	
Attack	
Evidence	1522805485
Other Info	1522805485, which evaluates to: 2018-04-04 03:31:25
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 11:01:03
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1540483477
Other Info	1540483477, which evaluates to: 2018-10-25 18:04:37
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-06 01:07:05
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1546045734
Other Info	1546045734, which evaluates to: 2018-12-29 03:08:54
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1548603684
Other Info	1548603684, which evaluates to: 2019-01-27 17:41:24

URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1549556828
Other Info	1549556828, which evaluates to: 2019-02-07 18:27:08
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 17:08:12
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1575990012
Other Info	1575990012, which evaluates to: 2019-12-10 17:00:12
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1595750129
Other Info	1595750129, which evaluates to: 2020-07-26 09:55:29
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1604231423
Other Info	1604231423, which evaluates to: 2020-11-01 13:50:23
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	

Evidence	1607167915
Other Info	1607167915, which evaluates to: 2020-12-05 13:31:55
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1609899400
Other Info	1609899400, which evaluates to: 2021-01-06 04:16:40
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1654270250
Other Info	1654270250, which evaluates to: 2022-06-03 17:30:50
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1687547391
Other Info	1687547391, which evaluates to: 2023-06-23 22:09:51
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1687895376
Other Info	1687895376, which evaluates to: 2023-06-27 22:49:36
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1694076839
Other Info	1694076839, which evaluates to: 2023-09-07 11:53:59
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET

Parameter	
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 07:21:40
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1700485571
Other Info	1700485571, which evaluates to: 2023-11-20 15:06:11
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1714657791
Other Info	1714657791, which evaluates to: 2024-05-02 16:49:51
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1724754687
Other Info	1724754687, which evaluates to: 2024-08-27 13:31:27
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1731405415
Other Info	1731405415, which evaluates to: 2024-11-12 11:56:55
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 03:23:13

URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1735328473
Other Info	1735328473, which evaluates to: 2024-12-27 21:41:13
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 03:29:39
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1750603025
Other Info	1750603025, which evaluates to: 2025-06-22 17:37:05
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1768516095
Other Info	1768516095, which evaluates to: 2026-01-16 00:28:15
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1770035416
Other Info	1770035416, which evaluates to: 2026-02-02 14:30:16
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	

Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 19:01:43
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1784335871
Other Info	1784335871, which evaluates to: 2026-07-18 03:51:11
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1802195444
Other Info	1802195444, which evaluates to: 2027-02-09 19:50:44
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1804477439
Other Info	1804477439, which evaluates to: 2027-03-08 05:43:59
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1804603682
Other Info	1804603682, which evaluates to: 2027-03-09 16:48:02
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1816402316
Other Info	1816402316, which evaluates to: 2027-07-24 07:11:56
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET

Parameter	
Attack	
Evidence	1836072691
Other Info	1836072691, which evaluates to: 2028-03-07 22:11:31
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1839030562
Other Info	1839030562, which evaluates to: 2028-04-11 03:49:22
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1856431235
Other Info	1856431235, which evaluates to: 2028-10-29 13:20:35
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 06:16:33
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1873313359
Other Info	1873313359, which evaluates to: 2029-05-12 23:49:19
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1887473919
Other Info	1887473919, which evaluates to: 2029-10-23 21:18:39

URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1894007588
Other Info	1894007588, which evaluates to: 2030-01-07 11:13:08
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 10:17:21
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1914138554
Other Info	1914138554, which evaluates to: 2030-08-28 12:09:14
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-02 01:59:48
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 21:43:42
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	

Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 20:17:31
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1994146192
Other Info	1994146192, which evaluates to: 2033-03-11 11:29:52
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 16:29:46
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	2003034995
Other Info	2003034995, which evaluates to: 2033-06-22 09:36:35
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	2005441023
Other Info	2005441023, which evaluates to: 2033-07-20 05:57:03
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	2007800933
Other Info	2007800933, which evaluates to: 2033-08-16 13:28:53
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET

Parameter	
Attack	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 05:20:15
URL	https://discord.com/assets/66635.1ad04eeb540c570d5e05.js
Method	GET
Parameter	
Attack	
Evidence	1540483477
Other Info	1540483477, which evaluates to: 2018-10-25 18:04:37
URL	https://discord.com/cdn-cgi/challenge-platform/h/b/scripts/jsd/bcc5fb0a8815/main.js
Method	GET
Parameter	
Attack	
Evidence	1712852971
Other Info	1712852971, which evaluates to: 2024-04-11 18:29:31
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnIcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5Ihvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3Ise:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b

	;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 07:37:29
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5Ihvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6Jlc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3Ise:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 03:23:13
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAAME6AcAAAAAAAAA

URL	AAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5Ihvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3Ise:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 06:16:33
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5Ihvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlh

URL	my;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1404277552
Other Info	1404277552, which evaluates to: 2014-07-02 07:05:52
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;

URL	kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1423857449
Other Info	1423857449, which evaluates to: 2015-02-13 21:57:29
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sY

	EX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1426400815
Other Info	1426400815, which evaluates to: 2015-03-15 08:26:55
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1454621731
Other Info	1454621731, which evaluates to: 2016-02-04 23:35:31

URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1466479909
Other Info	1466479909, which evaluates to: 2016-06-21 05:31:49
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb

URL	,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1483230225
Other Info	1483230225, which evaluates to: 2017-01-01 02:23:45
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mp

URL	EAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1504918807
Other Info	1504918807, which evaluates to: 2017-09-09 03:00:07
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hs

URL	LsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1510334235
Other Info	1510334235, which evaluates to: 2017-11-10 19:17:15
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,

	aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1541320221
Other Info	1541320221, which evaluates to: 2018-11-04 10:30:21
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1555261956

Other Info	1555261956, which evaluates to: 2019-04-14 19:12:36
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1567103746
Other Info	1567103746, which evaluates to: 2019-08-29 20:35:46
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/

	excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1591671054
Other Info	1591671054, which evaluates to: 2020-06-09 04:50:54
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:T

URL	ia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1594198024
Other Info	1594198024, which evaluates to: 2020-07-08 10:47:04
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;e

URL	BAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1622183637
Other Info	1622183637, which evaluates to: 2021-05-28 08:33:57
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:K

	UM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1634467795
Other Info	1634467795, which evaluates to: 2021-10-17 12:49:55
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	

Evidence	1658658271
Other Info	1658658271, which evaluates to: 2022-07-24 12:24:31
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1661365465
Other Info	1661365465, which evaluates to: 2022-08-24 20:24:25
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hs

URL	m,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/ excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/ m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1684777152
Other Info	1684777152, which evaluates to: 2023-05-22 20:39:12
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25

URL	sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1706088902
Other Info	1706088902, which evaluates to: 2024-01-24 11:35:02
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;c

URL	FTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1711684554
Other Info	1711684554, which evaluates to: 2024-03-29 05:55:54
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;

	wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1742555852
Other Info	1742555852, which evaluates to: 2025-03-21 13:17:32
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	

Attack	
Evidence	1759359992
Other Info	1759359992, which evaluates to: 2025-10-02 02:06:32
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1762050814
Other Info	1762050814, which evaluates to: 2025-11-02 04:33:34
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAA

	AAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1789927666
Other Info	1789927666, which evaluates to: 2026-09-20 21:07:46
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqt

URL	e:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1802195444
Other Info	1802195444, which evaluates to: 2027-02-09 19:50:44
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUe

URL	zZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1812370925
Other Info	1812370925, which evaluates to: 2027-06-07 15:22:05
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry

URL	6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1843258603
Other Info	1843258603, which evaluates to: 2028-05-30 03:16:43
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET

Parameter	
Attack	
Evidence	1852507879
Other Info	1852507879, which evaluates to: 2028-09-14 04:31:19
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1873836001
Other Info	1873836001, which evaluates to: 2029-05-19 01:00:01

URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1886057615
Other Info	1886057615, which evaluates to: 2029-10-07 11:53:35
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb

URL	,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1907459465
Other Info	1907459465, which evaluates to: 2030-06-12 04:51:05
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mp

URL	EAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1913087877
Other Info	1913087877, which evaluates to: 2030-08-16 08:17:57
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hs

URL	LsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1943803523
Other Info	1943803523, which evaluates to: 2031-08-06 20:25:23
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,

	aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1957810842
Other Info	1957810842, which evaluates to: 2032-01-15 22:20:42
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1969922972

Other Info	1969922972, which evaluates to: 2032-06-04 03:49:32
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1994146192
Other Info	1994146192, which evaluates to: 2033-03-11 11:29:52
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/

	excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	1996959894
Other Info	1996959894, which evaluates to: 2033-04-13 01:04:54
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:T

	ia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	2013776290
Other Info	2013776290, which evaluates to: 2033-10-24 17:18:10
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 07:37:29
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 03:23:13
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET

Parameter	
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 06:16:33
URL	https://discord.com/cdn-cgi/challenge-platform/h/b/jsd/r/872cb0975e860fd6
Method	POST
Parameter	Set-Cookie
Attack	
Evidence	1712856479
Other Info	1712856479, which evaluates to: 2024-04-11 19:27:59
Instances	201
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://127.0.0.1:2005/
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/@brikaasdev0096
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/admin
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/admin/challenges/create
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/admin/contests
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/admin/contests/create

Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/admin/contests/update/24
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/api/v1/piston/versions
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/api/v2/piston/runtimes
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/challenges
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/challenges/44/python
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/challenges/choose_language/44
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/contests
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/contests/disallowed_languages/24
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	x-content-type-options

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://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/41.bundle.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/5.bundle.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/9242107df7da7c6ad3cadf3133abcd37.ttf
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	x-content-type-options

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://127.0.0.1:2005/lib/webpack/main.bundle.css?1712848969921
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.css?1712856829510
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.css?1712856884638
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.css?1712856924268
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.css?1712857323608
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	x-content-type-options

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://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856829510
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856884638
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856924268
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/react.bundle.js?1712857323608
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/s/ROjOXc
Method	GET
Parameter	x-content-type-options

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://127.0.0.1:2005/snippets
Method	GET
Parameter	x-content-type-options
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://use.fontawesome.com/releases/v5.2.0/css/all.css
Method	GET
Parameter	x-content-type-options
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://use.fontawesome.com/releases/v5.2.0/webfonts/fa-solid-900.woff2
Method	GET
Parameter	x-content-type-options
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://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	x-content-type-options
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://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	x-content-type-options
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://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	x-content-type-options
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://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	x-content-type-options
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://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	x-content-type-options
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://127.0.0.1:2005/challenges/execute/44
Method	POST
Parameter	x-content-type-options

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://127.0.0.1:2005/snippets
Method	POST
Parameter	x-content-type-options
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://play.google.com/log?format=json&hasfast=true
Method	POST
Parameter	x-content-type-options
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	58
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	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://discord.com/api/v9/auth/login
Method	POST

Parameter	login
Attack	
Evidence	password
Other Info	userParam=login userValue=brikaaomar@gmail.com passwordParam=password referer=https://discord.com/login?redirect_to=%2Foauth2%2Fauthorize%3Fclient_id%3D496807648289882112%26redirect_uri%3Dhttp%253A%252F%252F127.0.0.1%253A2005%252Fauth%252Fdiscord_cb%26response_type%3Dcode%26scope%3Didentify%2520email
Instances	1
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/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Example Informational Alert Notification**
Description	An example alert - this description will usually have more useful information in it!
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	60200

Informational	**GET for POST**
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	
Attack	

Evidence	GET http://127.0.0.1:35769/AlertNotifications?anticsrf=74dc4328-9aef-4382-b8be-0e649cb3580a&key=68354094 HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Break?number=ZAP HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Comments?anticsrf=76a526c7-3aa1-4958-ab14-6be4ec3d2a1c&key=81088082 HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Enable?field1=ZAP&field2=ZAP&field3=ZAP HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Frames?anticsrf=b85c40c7-dc8e-4ac8-a5f8-546a11d59502&key=26149440 HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/History?anticsrf=4ca17d68-53f7-493f-8e58-4255657f971f&key=49781165 HTTP/1.1
Other Info	

URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/PageAlerts?anticsrf=b0e06a84-364d-4cd7-bfa6-64e1cc8d4309&key=54663771 HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Scope?anticsrf=a0e573a0-79ef-43fa-ac60-00695735cc13 HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Show?field2=ZAP&field3=ZAP&field4=ZAP HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/SiteAlerts?anticsrf=e0cc4f1b-f308-49ac-9d64-ccb036edc9ce&key=13279531 HTTP/1.1
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	
Attack	
Evidence	GET http://127.0.0.1:35769/Sites?anticsrf=6d2855cc-77db-424e-be69-014baeeba17a&key=70111060 HTTP/1.1
Other Info	
Instances	11
Solution	Ensure that only POST is accepted where POST is expected.

Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

Informational	**HUD Tutorial Page Alert**
Description	Alerts are usually potential security vulnerabilities that have been found in the target site. In this case, the alert is for the HUD tutorial, and the key you need is: 54663771
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	
CWE Id	
WASC Id	
Plugin Id	60200

Informational	**Information Disclosure - Sensitive Information in URL**
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://discord.com/api/v9/users/@me?with_analytics_token=true
Method	GET
Parameter	with_analytics_token
Attack	
Evidence	with_analytics_token
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: token with_analytics_token
URL	https://www.google.com/complete/search?q&cp=0&client=gws-wiz-serp&xssi=t&gs_pcrt=2&hl=ar&authuser=0&psi=4SMYZoekC5OjhbIPu4WF0AE.1712858082729&dpr=1.25&nolsbt=1
Method	GET
Parameter	authuser
Attack	
Evidence	authuser

Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user authuser
URL	https://www.google.com/complete/search?q=CVE-2019-8331&cp=0&client=desktop-gws-wiz-on-focus-serp&xssi=t&gs_pcrt=3&hl=ar&authuser=0&pq=CVE-2019-8331&psi=4SMYZoekC5OjhbIPu4WF0AE.1712858082729&dpr=1.25&ofp=EAEYqZLkpqTji5I9GN6n1M-yoebygAEYs93WxLTzmLTWARj9-PTH_4D3-ZYBGNeU3Z-I49m6HDKXAQoXChVjdmUtMjAxOS04MzMxIGV4cGxvaXQKEAoOQ1ZFLTIwMTktMTEzNTgKEAoOQ1ZFLTIwMjEtNDExODQKEAoOQ1ZFLTIwMjAtMjMwNjQKDwoNQ1ZFLTIwMTUtOTI1MQoQCg5DVkUtMjAyMC0xMTAyMwoQCg5DVkUgMjAxNiAxMDczNQoPCg1DVkUtMjAxNi03MTAzEEc
Method	GET
Parameter	authuser
Attack	
Evidence	authuser
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user authuser
Instances	3
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

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://127.0.0.1:2005/
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'0', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/@brikaasdev0096
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/admin
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/admin/challenges/create
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	
Attack	
Evidence	username

Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', '', see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/admin/contests/create
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', '', see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', '', see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'0', '', see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/challenges/44/python
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', '', see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/challenges/choose_language/44
Method	GET
Parameter	
Attack	

Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'0', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'0', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	

Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "! function(a,b){"use strict";"function"==typeof define&&define.amd? define(["jquery"],b):"object"==typeof exports?module.exports=b", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "! function(t,e){"object"==typeof exports&&"undefined"!=typeof module? e(exports,require("jquery"),require("popper.js")):"function"", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: "! function(e){var n="object"==typeof window&&window||"object"==typeof self&&self;"undefined"! =typeof exports?e(exports):n&&(n.hlj", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 2 times, the first in the element starting with: "return j.call(r(a),c)})),b))for(;i>h;h++)b(a[h],c,g?d:d.call(a[h],h,b(a[h],c)));return e? a:j?b.call(a):i?b(a[0],c):f},T=function", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "! function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=a.document?b(a,!0):function(", see evidence field for the suspicious comment/ snippet.

URL	http://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"f", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/41.bundle.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"c", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/5.bundle.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"c", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	
Attack	
Evidence	Debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "/*! exports provided: StringDiffSequence, stringDiff, Debug, MyArray, LcsDiff */", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	
Attack	

Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 8 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"E", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"U", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"S", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"R", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"t", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 31 times, the first in the element starting with: "eval("\nvar NATIVE_ARRAY_BUFFER = __webpack_require__(/*! ../internals/array-buffer-native */ \"./node_modules/core-js/internals", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar global = __", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval("\nvar fixRegExpWellKnownSymbolLogic = __webpack_require__(/*! ../internals/fix-regexp-well-known-symbol-logic */ \"./node_", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 30 times, the first in the element starting with: "/******/ // add entry modules from loaded chunk to deferred list", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "eval("\n\nexports.byteLength = byteLength\nexports.toByteArray = toByteArray\nexports.fromByteArray = fromByteArray\n\nvar looku", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 10 times, the first in the element starting with: "eval("/* WEBPACK VAR INJECTION */(function(global) {/*!\n * The buffer module from node.js, for the browser.\n *\n * @author F", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 11 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\n\n// Headers whose duplicat", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\nvar settle = __webpack_requ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar isObject = ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 31 times, the first in the element starting with: "eval("\nvar NATIVE_ARRAY_BUFFER = __webpack_require__(/*! ../internals/array-buffer-native */ \"./node_modules/core-js/internals", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	

Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar global = __", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval("\nvar fixRegExpWellKnownSymbolLogic = __webpack_require__(/*! ../internals/fix-regexp-well-known-symbol-logic */ \"./node_", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 30 times, the first in the element starting with: "/******/ // add entry modules from loaded chunk to deferred list", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "eval("\n\nexports.byteLength = byteLength\nexports.toByteArray = toByteArray\nexports.fromByteArray = fromByteArray\n\nvar looku", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 10 times, the first in the element starting with: "eval("/* WEBPACK VAR INJECTION */(function(global) {/*!\n * The buffer module from node.js, for the browser.\n *\n * @author F", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 11 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\n\n// Headers whose duplicat", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\nvar settle = __webpack_requ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar isObject = ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	

Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 31 times, the first in the element starting with: "eval("\nvar NATIVE_ARRAY_BUFFER = __webpack_require__(/*! ../internals/array-buffer-native */ \"./node_modules/core-js/internals", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar global = __", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval("\nvar fixRegExpWellKnownSymbolLogic = __webpack_require__(/*! ../internals/fix-regexp-well-known-symbol-logic */ \"./node_", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 30 times, the first in the element starting with: "/******/ // add entry modules from loaded chunk to deferred list", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "eval("\n\nexports.byteLength = byteLength\nexports.toByteArray = toByteArray\nexports.fromByteArray = fromByteArray\n\nvar looku", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 10 times, the first in the element starting with: "eval("/* WEBPACK VAR INJECTION */(function(global) {/*!\n * The buffer module from node.js, for the browser.\n *\n * @author F", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 11 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\n\n// Headers whose duplicat", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	

Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\nvar settle = __webpack_requ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar isObject = ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 31 times, the first in the element starting with: "eval("\nvar NATIVE_ARRAY_BUFFER = __webpack_require__(/*! ../internals/array-buffer-native */ \"./node_modules/core-js/internals", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar global = __", see evidence field for the suspicious comment/

	snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval("\nvar fixRegExpWellKnownSymbolLogic = __webpack_require__(/*! ../internals/fix-regexp-well-known-symbol-logic */ \"./node_", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 30 times, the first in the element starting with: "/******/ // add entry modules from loaded chunk to deferred list", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "eval("\n\nexports.byteLength = byteLength\nexports.toByteArray = toByteArray\nexports.fromByteArray = fromByteArray\n\nvar looku", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	

Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 10 times, the first in the element starting with: "eval("/* WEBPACK VAR INJECTION */(function(global) {/*!\n * The buffer module from node.js, for the browser.\n *\n * @author F", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 11 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\n\n// Headers whose duplicat", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\nvar settle = __webpack_requ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar isObject = ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the

	suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 31 times, the first in the element starting with: "eval("\nvar NATIVE_ARRAY_BUFFER = __webpack_require__(/*! ../internals/array-buffer-native */ \"./node_modules/core-js/internals", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar global = __", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval("\nvar fixRegExpWellKnownSymbolLogic = __webpack_require__(/*! ../internals/fix-regexp-well-known-symbol-logic */ \"./node_", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 30 times, the first in the element starting with: "/******/ // add entry modules from loaded chunk to deferred list", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	

Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "eval("\n\nexports.byteLength = byteLength\nexports.toByteArray = toByteArray\nexports.fromByteArray = fromByteArray\n\nvar looku", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var react__WEBPACK_IMPORTED_MODULE_0__ = __webpack_requi", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 10 times, the first in the element starting with: "eval("/* WEBPACK VAR INJECTION */(function(global) {/*!\n * The buffer module from node.js, for the browser.\n *\n * @author F", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 11 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\n\n// Headers whose duplicat", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "eval("\n\nvar utils = __webpack_require__(/*! ./../utils */ \"./node_modules/axios/lib/utils.js\");\nvar settle = __webpack_requ", see evidence field for the

	suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: "eval("\nvar $ = __webpack_require__(/*! ../internals/export */ \"./node_modules/core-js/internals/export.js\");\nvar isObject = ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 6 times, the first in the element starting with: "eval("exports = module.exports = __webpack_require__(/*! ../../../../../../../css-loader/dist/runtime/api.js */ \"./node_modules", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"M", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	Debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 4 times, the first in the element starting with: "eval("exports = module.exports = __webpack_require__(/*! ../../../../../../../css-loader/dist/runtime/api.js */ \"./node_modules", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 52 times, the first in the element starting with: "eval("exports = module.exports = __webpack_require__(/*! ../../../../../../../css-loader/dist/runtime/api.js */ \"./node_modules", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 4 times, the first in the element starting with: "/******/ // create error before stack unwound to get useful stacktrace later", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 8 times, the first in the element starting with: "eval("\n\n/*\n MIT License http://www.opensource.org/licenses/mit-license.php\n Author Tobias Koppers @sokra\n*/\n// css base ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected 17 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"c", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 33 times, the first in the element starting with: "eval("exports = module.exports = __webpack_require__(/*! ../../../../../../../css-loader/dist/runtime/api.js */ \"./node_modules", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 37 times, the first in the element starting with: "eval("exports = module.exports = __webpack_require__(/*! ../../../../../../../css-loader/dist/runtime/api.js */ \"./node_modules", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 26 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"S", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval("/** @license React v16.12.0\n * react-dom.development.js\n *\n * Copyright (c) Facebook, Inc. and its affiliates.\n *\n * ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856829510
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval("/** @license React v16.12.0\n * react-dom.development.js\n *\n * Copyright (c) Facebook, Inc. and its affiliates.\n *\n * ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856884638
Method	GET
Parameter	

Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval("/** @license React v16.12.0\n * react-dom.development.js\n *\n * Copyright (c) Facebook, Inc. and its affiliates.\n *\n * ", see evidence field for the suspicious comment/ snippet.
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856924268
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval("/** @license React v16.12.0\n * react-dom.development.js\n *\n * Copyright (c) Facebook, Inc. and its affiliates.\n *\n * ", see evidence field for the suspicious comment/ snippet.
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712857323608
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval("/** @license React v16.12.0\n * react-dom.development.js\n *\n * Copyright (c) Facebook, Inc. and its affiliates.\n *\n * ", see evidence field for the suspicious comment/ snippet.
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	
Attack	
Evidence	Debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "/*! exports provided: StringDiffSequence, stringDiff, Debug, MyArray, LcsDiff */", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 8 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"E", see evidence field for the suspicious comment/snippet.

URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"U", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"S", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"R", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 5 times, the first in the element starting with: "eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */ __webpack_require__.d(__webpack_exports__, \"t", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/s/ROjOXc
Method	GET
Parameter	

Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "<script> ctx = { cdn_url: 'https://127.0.0.1:2005/cdn', user_id: +'1', ", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/07b3122d5031b91257f3.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["25381"], {255963:function(t,e,i){"use strict";t.exports=i", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/10586.3f509a5d474354a36c24.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["10586"], {772425:function(t,r,n){"use strict";var e=n("93", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/11250.635085824b0937a12098.js
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["11250"], {725436:function(e,t,a){"use strict";a.r(t),a.d(", see evidence field for the suspicious comment/snippet.

URL	https://discord.com/assets/17764.2aa7ee221234529f6e80.js
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["17764"], {540571:function(t,n,e){"use strict";e.r(n),e.d(", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/200944d085aeab393864.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "! function(){var t,r,e={610148:function(t,r,e){"use strict";var n=e("325008"),o=e("498576"),i=TypeError,u=Object.getOwnPropertyDe", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/43455.8c79ce3e1753b38de4a4.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 5 times, the first in the element starting with: "Reason: ${t}`)})}_process(t){this._numProcessing+ +,t.then(t=>(this._numProcessing--,t),t=>(this._numProcessing--,t))}_sendEnvelo", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/43455.8c79ce3e1753b38de4a4.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 4 times, the first in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app|| []).push([["43455"],{903204:function(t,e,n){"use strict";n.r(e),n.d(", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/4ae7208f1a5879907bb7.js
Method	GET
Parameter	

Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["90212"], {292824:function(e,t,n){"use strict";e.exports=n", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/4fba8c74f8389fc6739c.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["2047"], {848304:function(e,t,n){"use strict";e.exports=n.", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/52030.51d5c15949ffbbbfa744.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["52030"], {48550:function(e,t,s){"use strict";s.r(t),s.d(t", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/56a5e5a759d087feebf0.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["92223"], {331650:function(e,s,t){"use strict";t.r(s);var ", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/57878.f80f2ae72af75d9274b1.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["57878"], {981632:function(t,e,n){"use strict";n.r(e),n.d(", see evidence field for the suspicious comment/

	snippet.
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["58661"], {946188:function(e,t,n){"use strict";n.r(t);var ", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: "`.replace(/\s*\/\/.*$/gm,"").replace(/\n/g,"").trim(),o=e=>e&&e.exact?RegExp(`(?:^${r}$)\|(?:^${a} $)`):RegExp(`(?:${n(e)}${r}${n(", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/65573.71e278ef7f5773eb2c7b.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["65573"], {290034:function(e,t,n){var i={"./bg.jsona":func", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/66635.1ad04eeb540c570d5e05.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["66635"], {473452:function(e,t,n){"use strict";n.r(t);t.de", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/67535.a3d024cb667257cc4585.js
Method	GET
Parameter	

Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["67535"], {533307:function(e,t,l){"use strict";let n;l.r(t", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/84471.7c0676f47681e985acbc.js
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["84471"], {981631:function(_,E,e){"use strict";e.r(E),e.d(", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/85514.4384a756cb8409699d33.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["85514"], {379760:function(e,t,s){"use strict";s.r(t),s.d(", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/86691.5616f1f9bb62628b6533.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["86691"], {515695:function(e,t,n){"use strict";e.exports=n", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/87dc123baf1996fe4423.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["58153"], {280501:function(e,t,l){"use strict";var n,a,u,i", see evidence field for the suspicious comment/

	snippet.
URL	https://discord.com/assets/90687.8573be403cf58ebc2a36.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["90687"], {231443:function(e,t,n){"use strict";e.exports=n", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/98b772b4782208b1374c.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["79504"], {943702:function(e,t,n){"use strict";e.exports=n", see evidence field for the suspicious comment/ snippet.
URL	https://discord.com/assets/app.22eae750ddb12b089c65.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["99387"], {823734:function(e){"use strict";e.exports={addF", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/c0e599a3aaf92f662139.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["95393"], {392459:function(e){"use strict";e.exports="data", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/e16904bc61f4a8561939.js
Method	GET
Parameter	

Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["10778"], {418757:function(e,s,a){"use strict";e.exports=a", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/e66e5fa5777216466869.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["83081"], {70519:function(e,t,s){"use strict";e.exports=s.", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/f7eee8828b39e32d39bc.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["46369"], {631274:function(e,t,n){"use strict";e.exports=n", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/shared.54491af62d8ce9108c2b.js
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "(this.webpackChunkdiscord_app=this.webpackChunkdiscord_app||[]).push([["49237"], {996176:function(e){"use strict";e.exports={anch", see evidence field for the suspicious comment/snippet.
URL	https://discord.com/assets/web.288209e041528862eb8f.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "!function(){var e,t,a,d,n,c,i,o,r,f={799656:function(e,t,a){"use strict";a.r(t);var d=a("735250");a("470079");var n=a("613828"),", see evidence field for the suspicious comment/

	snippet.
URL	https://discord.com/cdn-cgi/challenge-platform/h/b/scripts/jsd/bcc5fb0a8815/main.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "window._cf_chl_opt={cFPWv:'b'};~function(V,g,h,i,j,k,o,s){V=b,function(c,e,U,f,C){for(U=b,f=c();!![];)try{if(C=parseInt(U(500))/", see evidence field for the suspicious comment/snippet.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 5 times, the first in the element starting with: "function hf(a,b){var c=gf[a];c&&J(c);"displayFeaturesTask"===a&&void 0==b&&J(96);/.*Task$/.test(a)&&J(92)}function mf(a,b){if(a)", see evidence field for the suspicious comment/snippet.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "function Pe(a){try{if(!a.get(Qe)&&(a.set(Qe,!0),!a.get("&gtm"))){var b=void 0,c=void 0;If(be("gtm_debug"))&&(b=2);!b&&D(M.referr", see evidence field for the suspicious comment/snippet.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 5 times, the first in the element starting with: "c=0>c?a.href:a.href.substr(0,c));a=c;break;case "protocol":a=d;break;case "host":a=a.hostname.replace(N,"").toLowerCase();c&&(c=", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAAB

	AAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=sy3tf,sy483,w4UyN,syx8,syx9,EbPKJf,sy4nm,sy6x3,J9Q59e,sy4nn,a6Sgfb,Tia57b,KpRAue,sy14u,NyeqM,sy2nk,sy2nl,O9SqHb?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "ASg(a,b),d=c?a.oa.get(c):void 0;return((null==d?0:d.omit)?BSg(d.omit):[]).find(function(e){return"function"===typeof e?e(b):a.is", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=sy3tf,sy483,w4UyN,syx8,syx9,EbPKJf,sy4nm,sy6x3,J9Q59e,sy4nn,a6Sgfb,Tia57b,KpRAue,sy14u,NyeqM,sy2nk,sy2nl,O9SqHb?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "_.Smc=function(a){if(!a.match(/.*com\/search|^\/search/))return _.id(new _.Ud("url invalid not / search")),{SNa:!1,vxd:!0};var b,", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected 9 times, the first in the element starting with: "_.PDb=function(a){this.la=_.n(a)};_.F(_.PDb,_.p);_.QDb=function(a,b){return _.zj(a,1,b)};_.RDb=function(a,b){return _.zj(a,2,b)}", see evidence field for the suspicious comment/snippet.

URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: "var n0f,o0f,p0f,q0f;n0f=_.Hg(["@-webkit-keyframes mspin{from{-webkit-transform:translateX(0);}to{-webkit-transform:translateX(-1", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "var V6b=function(a,b,c){var d=b==a.wa|| b&&a.wa&&b.getFullYear()==a.wa.getFullYear()&&b.getMonth()==a.wa.getMonth(),e=b==a.wa|| d&", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbM

	T3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 31 times, the first in the element starting with: "var baa,caa,laa,naa,oaa,paa,qaa,raa,saa,taa,uaa,vaa,zaa,xaa,waa,Aaa,yaa,Baa,Daa,Caa,Eaa,Faa,Gaa,Iaa,Raa,Waa,iba,oba,xba,zba,Dba,", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5Ihvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:

URL	sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "_.Be.set("debug.apply-debug-flags",_.qo("CgIzTb"));_.Be.set("debug.refresh-path-quality-metric",_.qo("U8qUPd"));_.Be.set("debug.", see evidence field for the suspicious comment/ snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 49 times, the first in the element starting with: "c,d,e)})}catch(g){}};fja=function(a){var b=new Set;if(a.stack) {a=a.stack.toString().matchAll(/https:\/\/[^:]+/g);a=_.Za(a);for(v", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 9 times, the first in the element starting with: "a[g+3]<<24;case 3:b+=a[g+2]<<16;case 2:b+=a[g+1]<<8;case 1:b+=a[g]} h();return rGa.toString(d)};sGa=function(a){for(var b=[],c=0;", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/

URL	rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3Ise:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected 16 times, the first in the element starting with: "Jma=function(a){a=_.ze(a);var b=a.tagName.toUpperCase(),c=(a.getAttribute("role")||"").toUpperCase();return"BUTTON"===b|| "BUTTON", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOx

URL	d;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 4 times, the first in the element starting with: "a.message||"The request is not allowed by the user agent or the platform in the current context, possibly because the user denie", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MBykysAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/

	m=attn,cdos,gwc,hsm,jsa,mb4ZUb,d,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "_.Uc=function(a,b){var c=this;b=void 0===b?{}:b;var d=void 0===b.lPc?_.WDa:b.lPc;a=""===a?[]:_.xm(a);b=a[1]||"";this.protocol=b+", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	

Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 3 times, the first in the element starting with: "_.Ytg=function(a,b){return _.Re(a,8,b)};_.Ztg=function(){var a=new _.hxc;return _.zj(a,2,2)};_.$tg=function(a,b){return _.Mb(a,_", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected 11 times, the first in the element starting with: "width:Q.Qc(),height:Q.Hc(),Ula:3})),null!=(ma=b)&&null!=(ua=ma.dga())&&null!=(Da=_.t(ua,_.Aw,4))&&_.ag(Da,29));if("undefined"!==", see evidence field for the suspicious comment/snippet.

URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 22 times, the first in the element starting with: "b+"): "+sCu(a,c)+(d?" "+d:"")})},uCu=function(a,b){a.info(function(){return"TIMEOUT: "+b})};pCu.prototype.debug=function(){};pCu", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hs

URL	m,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/ excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/ m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 17 times, the first in the element starting with: "_F_installCss(".jbBItf{display:block;position:relative}.DU0NJ{bottom:0;right:0;position:absolute;left:0;top:0}.IP3Jof{display:in", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:

URL	MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RoITY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	Query
Other Info	The following pattern was used: \bQUERY\b and was detected 13 times, the first in the element starting with: "_.l.Vx=function(){return this.Cb};_.l.cancel=function(){if("Response received"!=this.Je&&"Error"!=this.Je){this.Gm.removeAll();t", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tlj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlh

URL	my;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element starting with: "sv.set("sc_sc",_.qo("OW9R3e"));sv.set("scc_ir",_.qo("A8F2wc"));sv.set("scc_iu",_.qo("NdNKIc"));sv.set("scc_ou",_.qo("nUQosc"));s", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;e

URL	BAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=EO13pd,EkevXb,GU4Gab,Gg40M,MpJwZc,PbHo4e,RJ1Nyd,RagDlc,T5VV,UUJqVe,Wo3n8,aDVF7,aa,abd,async,bgd,epYOx,foot,gOTY1,kyn,lli,mu,ogmBcd,q0xTif,rhYw1b,s39S4,sOXFj,sYEX8b,sb_wiz,sf,spch,tl?xjs=s2
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "fKb.prototype.Ta=function(){hKb(this,!1)};var hKb=function(a,b){if(!a.oa||!_.We(a.PD,9)|| a.model.getState().OWa()===_.We(a.PD,9)", see evidence field for the suspicious comment/ snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;

	vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tIj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 8 times, the first in the element starting with: "_.wOd=function(){this.oa=vOd("&a&0&0trk9--nx?27qjf--nx?e9ebgn--nx?nbb0c7abgm--nx??1&2oa08--nx?apg6qpcbgm--nx?hbbgm--nx?rdceqa08-", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tIj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	

Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected 10 times, the first in the element starting with: "h)===d&&(f=g.length-1)):"$sd"==k[0]&&(g.push(h),-1==f&&(f=g.length-1)),h=M2d(h);d=g.length ;for(h=0;h<d;++h){k=h==f;var m=c[h];k|", see evidence field for the suspicious comment/ snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/ am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAA QAEACVgGyEKAAQQDAABCCAH7- FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAg GwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAA AAAAAAAAABAKp24PAQASA/d=1/ exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/ excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTIc,PoJj 8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb ,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2d Qd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX 2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ: MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqt e:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUd b;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25 sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:T ia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVIQ Od;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mp EAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlh my;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fT fGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46 d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:Yquh Tb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUe zZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE 9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;c FTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;e BAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;ga ub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hs LsYc:VI118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe; kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAu c:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9 Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQ zcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry 6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c; vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte; wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:K UM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/ m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tlj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "b(a.lc);SG.$vs=b(a.Pl);SG.$c.hE=1;SG.display.hE=1;SG.$if.hE=1;SG. $sk.hE=1;SG["for"].hE=4;SG["for"].ka=2;SG.$fk.hE=4;SG.$fk.ka=2;", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/ am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAA QAEACVgGyEKAAQQDAABCCAH7-

URL	FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tIj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 9 times, the first in the element starting with: "}else throw Error("Kd");}return c};Pq.prototype.Ta=function(a,b,c,d){var e=_.La(c),f=_.La(d);return a[e]<a[f]?1:a[e]>a[f]?-1:c.i", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:

	MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tIj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	
Evidence	QUERY
Other Info	The following pattern was used: \bQUERY\b and was detected 3 times, the first in the element starting with: "FUg.prototype.getDescriptor=function(){var a=GUg;a||(GUg=a=_.yE(FUg,{0: {name:"LocationDescriptor",fullName:"location.unified.Loc", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:Yquh

	Tb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tIj4fb,xdV1C?xjs=s1
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "k3d.prototype.apply=function(a){var b=a.nodeName;b="input"==b||"INPUT"==b||"option"==b||"OPTION"==b||"select"==b||"SELECT"==b||"", see evidence field for the suspicious comment/snippet.
URL	https://www.google.com/xjs/_/js/md=3/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "{"chunkTypes":"1000011111111001111000100001011010000001111111111111111111111111111111111111111111011110111111111111010111111111111111", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 10 times, the first in the element starting with: "aa.pop=function(){return this.m.pop()};aa.push=function(a){return this.m.push.apply(this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/snippet.

URL	https://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 4 times, the first in the element starting with: "var lh=function(a,b){for(var c=0;c<b.length;c++){if(void 0===a)return;a=a[b[c]]} return a},mh=function(a,b){var c=b.preHit;if(c){", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 11 times, the first in the element starting with: "case "port":f=String(Number(a.port)||("http"===g?80:"https"===g?443:"")));break;case "path":a.pathname||a.hostname||jb("TAGGING","", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "function ic(a){var b;if(a instanceof $b)if(a instanceof $b)b=a.Dj;else throw Error("");else b=hc.test(a)?a:void 0;return b};var ", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=G-N33Q40M7WG&l=dataLayer&cx=c
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&"code"!==e)throw c(d,{},"Unknown user provided data source.");if(b.vtp_limitDataSources)if("auto"!==e||b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	

Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 10 times, the first in the element starting with: "aa.pop=function(){return this.m.pop()};aa.push=function(a){return this.m.push.apply(this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 7 times, the first in the element starting with: "aa.pop=function(){return this.m.pop()};aa.push=function(a){return this.m.push.apply(this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: "function At(a,b){var c=void 0==Mb[3]?1:Mb[3],d='iframe[data-tagging-id="'+b+'"]',e=[];try{if(1===c){var f=D.querySelector(d);f&&", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: "function zt(a,b){var c=void 0==Lb[3]?1:Lb[3],d='iframe[data-tagging-id="'+b+'"]',e=[];try{if(1===c){var f=G.querySelector(d);f&&", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 10 times, the first in the element starting with: "case "port":f=String(Number(a.port)||("http"===g?80:"https"===g?443:""));break;case "path":a.pathname||a.hostname||ib("TAGGING",", see evidence field for the

	suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 10 times, the first in the element starting with: "case "port":f=String(Number(a.port)||("http"===g?80:"https"===g?443:""));break;case "path":a.pathname||a.hostname||jb("TAGGING",", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "function hc(a){var b;if(a instanceof Zb)if(a instanceof Zb)b=a.Dj;else throw Error("");else b=gc.test(a)?a:void 0;return b};var ", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "function ic(a){var b;if(a instanceof $b)if(a instanceof $b)b=a.Dj;else throw Error("");else b=hc.test(a)?a:void 0;return b};var ", see evidence field for the suspicious comment/snippet.
URL	https://www.googletagmanager.com/gtag/js?id=UA-28939284-9
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&"code"!==e)throw c(d,{},"Unknown user provided data source.");if(b.vtp_limitDataSources)if("auto"!==e||b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET

Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 9 times, the first in the element starting with: "var ja,ka,na,oa,sa,ua,va,wa,xa,Ha,Ia,Ja,La,Ma,Na,Qa,bb,ab,db,fb,eb,gb,hb,kb,ub,zb,Eb,Jb,Mb,Pb,Rb,Sb,Tb;_.ia=function(a,b){if(Err", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 9 times, the first in the element starting with: "typeof d.get)for(const f of d.keys())c.set(f,d.get(f));else throw Error("O`"+String(d));d=Array.from(c.keys()).find(f=>"content-", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: """></head><body><iframe id="'+a+'" name="'+a+'"></iframe>')): (a=Ln(b),a=_.ld('<body><iframe id="'+a+'" name="'+a+'"></iframe>'))", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: "var fq=function(a){const b=c=>encodeURIComponent(c).replace(/[!()~']|(%20)/g,d=>({"!":"%21","(":"%28",")":"%29","%20":"+","'":"%", see evidence field for the suspicious comment/snippet.
Instances	186
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	**Loosely Scoped Cookie**
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope.The domain scope applied to a cookie determines which domains can access it. For example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.
URL	https://adservice.google.com/adsid/google/si?gadsid=AORoGNRfzEOEOU6HVESnimbmzwWbmes6qJ1Dq5ge5O5Rn1CY2_x6WyhEB5AW
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: adservice.google.com ANID=AHWqTUlwsXKjPxyqeaYEwqmnj6dIH4KfHSa9VraPjmtqHOB9MnkR1h2ftHv1KBRg
URL	https://groups.google.com/group/zaproxy-hud
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: groups.google.com NID=513=LkSdvfv-yebxZFLt6DEIyzIt7orj3KlavmHcULUClmr9voYHru0bcja9fZo-Av5TSE3Yxfsk8LQcDPKVJwwgr-xCcVOHe9LXmnS5Bpjx3EgruSkkhU9N4G9kBDGFivGs3xAlwpA8nCpUJZOH0kZRIHQQPGQd7gGN0AG7e6jnzmU
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: www.google.com 1P_JAR=2024-04-11-17
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET
Parameter	
Attack	
Evidence	

Other Info	The origin domain used for comparison was: www.google.com 1P_JAR=2024-04-11-17 NID=513=hTstlQ33Fh8dPB3QwzYUZjfB8kV-wIg8CPlQIH_Yf6ONzyEVzBQZxROCduIYbug1pOwuQpMbdjCfeXJvp9sM4ZGlxdme2G-wfbLMmtClb2O5ntSDXPev0tCEgVtFYn_oqU_KdGvGE118bwjoyVtIquipiZSEGjGWG6w1HSHDYUdM80nVxnuBcWrr
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: www.google.com 1P_JAR=2024-04-11-17
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: www.google.com 1P_JAR=2024-04-11-17
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: www.google.com 1P_JAR=2024-04-11-17 AEC=AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg NID=513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: play.google.com NID=513=Fkhp3GTWS2SApZ3zxO5GyFQ7dxE02zAQ_kjbuvGYHTlExnc-OurKejpw0BB7nNH5_Gx_2W9ecARSaJghihS1C2A51rA-w_bLlGlx4DLHM0nLs1uqQ63a9qWvErmub4yk1SG__CvVFpHpkdMrDgp13zF1qFOQvZ9HFPJ7kO4pzk5hRDkmXkjP8Q
Instances	8
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).

Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
CWE Id	565
WASC Id	15
Plugin Id	90033

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://127.0.0.1:2005/
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/@brikaasdev0096
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/admin
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	
Attack	
Evidence	 Tools

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://127.0.0.1:2005/admin/challenges/create
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/admin/contests
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/admin/contests/create
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/admin/contests/update/24
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/challenges
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/challenges/44/python
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/challenges/choose_language/44
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/contests
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/s/ROjOXc
Method	GET
Parameter	
Attack	
Evidence	 Tools
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://127.0.0.1:2005/snippets
Method	GET

Parameter	
Attack	
Evidence	 Tools
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://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	
Attack	
Evidence	<script nonce="MTQxLDE3Niw0Miw0LDE0MCwyMjksMTQxLDIyMw==">window.GLOBAL_ENV = { API_ENDPOINT: '//discord.com/api', API_VERSION: 9, GATEWAY_ENDPOINT: 'wss://gateway.discord.gg', WEBAPP_ENDPOINT: '//discord.com', CDN_HOST: 'cdn.discordapp.com', ASSET_ENDPOINT: '//discord.com', MEDIA_PROXY_ENDPOINT: '//media.discordapp.net', WIDGET_ENDPOINT: '//discord.com/widget', INVITE_HOST: 'discord.gg', GUILD_TEMPLATE_HOST: 'discord.new', GIFT_CODE_HOST: 'discord.gift', RELEASE_CHANNEL: 'stable', DEVELOPERS_ENDPOINT: '//discord.com', MARKETING_ENDPOINT: '//discord.com', BRAINTREE_KEY: 'production_ktzp8hfp_49pp2rp4phym7387', STRIPE_KEY: 'pk_live_CUQtlpQUF0vufWpnpUmQvcdi', ADYEN_KEY: 'live_E3OQ33V6GVGTXOVQZEAFQJ6DJIDVG6SY', NETWORKING_ENDPOINT: '//router.discordapp.net', RTC_LATENCY_ENDPOINT: '//latency.discord.media/rtc', ACTIVITY_APPLICATION_HOST: 'discordsays.com', PROJECT_ENV: 'production', REMOTE_AUTH_ENDPOINT: '//remote-auth-gateway.discord.gg', SENTRY_TAGS: {"buildId":"f0ab68f22229d6b37665abe5d349d0a8613dcca6","buildType":"normal"}, MIGRATION_SOURCE_ORIGIN: 'https://discordapp.com', MIGRATION_DESTINATION_ORIGIN: 'https://discord.com', HTML_TIMESTAMP: Date.now(), ALGOLIA_KEY: 'aca0d7082e4e63af5ba5917d5e96bed0', PUBLIC_PATH: '/assets/' };</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	
Attack	
Evidence	التخطي إلى المحتوى الرئيسي
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	17
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://discord.com/api/v9/auth/location-metadata
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email&integration_type=0
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://discord.com/api/v9/users/@me?with_analytics_token=true
Method	GET
Parameter	cache-control
Attack	

Evidence	
Other Info	
URL	https://discord.com/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	cache-control
Attack	
Evidence	private
Other Info	
URL	https://www.google.com/async/bgasy?ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449&client=firefox-b-d&yv=3&cs=0&async=_fmt:jspb
Method	GET
Parameter	cache-control
Attack	
Evidence	private
Other Info	
URL	https://www.google.com/complete/search?q&cp=0&client=gws-wiz-serp&xssi=t&gs_pcrt=2&hl=ar&authuser=0&psi=4SMYZoekC5OjhbIPu4WF0AE.1712858082729&dpr=1.25&nolsbt=1
Method	GET
Parameter	cache-control
Attack	
Evidence	private, max-age=3600
Other Info	
URL	https://www.google.com/complete/search?q=CVE-2019-8331&cp=0&client=desktop-gws-wiz-on-focus-serp&xssi=t&gs_pcrt=3&hl=ar&authuser=0&pq=CVE-2019-8331&psi=4SMYZoekC5OjhbIPu4WF0AE.1712858082729&dpr=1.25&ofp=EAEYqZLkpqTji5I9GN6n1M-yoebygAEYs93WxLTzmLTWARj9-PTH_4D3-ZYBGNeU3Z-I49m6HDKXAQoXChVjdmUtMjAxOS04MzMxIGV4cGxvaXQKEAoOQ1ZFLTIwMTktMTEzNTgKEAoOQ1ZFLTIwMjEtNDExODQKEAoOQ1ZFLTIwMjAtMjMwNjQKDwoNQ1ZFLTIwMTUtOTI1MQoQCg5DVkUtMjAyMC0xMTAyMwoQCg5DVkUgMjAxNiAxMDczNQoPCg1DVkUtMjAxNi03MTAzEEc
Method	GET
Parameter	cache-control
Attack	
Evidence	no-cache, must-revalidate
Other Info	
URL	https://www.google.com/compressiontest/gzip.html

Method	GET
Parameter	cache-control
Attack	
Evidence	no-cache, must-revalidate
Other Info	
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	cache-control
Attack	
Evidence	private, max-age=0
Other Info	
URL	https://discord.com/api/v9/auth/login
Method	POST
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://discord.com/api/v9/auth/mfa/totp
Method	POST
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Parameter	cache-control
Attack	

Evidence	private
Other Info	
Instances	15
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	https://cdn.quilljs.com/1.0.0/quill.snow.css
Method	GET
Parameter	
Attack	
Evidence	Age: 177221
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdn.quilljs.com/1.0.0/quill.snow.css
Method	GET
Parameter	
Attack	
Evidence	Age: 183085
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh50XSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 32234
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.

URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh6UVSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 34927
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh6UVSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 40791
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh7USSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 589141
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/lato/v24/S6u9w4BMUTPHh7USSwiPGQ.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 595006
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/lato/v24/S6uyw4BMUTPHjx4wXg.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 585371
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/lato/v24/S6uyw4BMUTPHjx4wXg.woff2
Method	GET

Parameter	
Attack	
Evidence	Age: 591236
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/notonaskharabicui/v4/9XU6lIJqkU_PWDHIY3lkVjo6pdPHBQyThjcnXyA.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 40227
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://use.fontawesome.com/releases/v5.2.0/css/all.css
Method	GET
Parameter	
Attack	
Evidence	Age: 1308487
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://use.fontawesome.com/releases/v5.2.0/css/all.css
Method	GET
Parameter	
Attack	
Evidence	Age: 1314352
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://use.fontawesome.com/releases/v5.2.0/webfonts/fa-solid-900.woff2
Method	GET
Parameter	
Attack	
Evidence	Age: 5864
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Parameter	

Attack	
Evidence	Age: 1494
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Parameter	
Attack	
Evidence	Age: 158
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/og/_/js/k=og.asy.en_US.tu4jbdEqkHI.2019.O/rt=j/m=_ac,_awd,ada,lldp/exm=/d=1/ed=1/rs=AA2YrTtwQODFvUvyLaOY1jjUUg3IVWIMsg
Method	GET
Parameter	
Attack	
Evidence	Age: 101327
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/og/_/ss/k=og.asy.DzP_dblOEpw.R.F4.O/m=ll_tdm,adc,ll_fw/excm=/d=1/ed=1/ct=zgms/rs=AA2YrTsmw3C5zSuPckfjJ3sSxBCz1yduSA
Method	GET
Parameter	
Attack	
Evidence	Age: 100356
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	17
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://127.0.0.1:2005/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AA64eAgqV86JpEBoMW4cLfGica56li11m.gX%2Fj1EIWogv6jK%2Bi%2BBLzL76cGgM5bTjW00GhJfrL9XQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AudQUKCj4HJc_LhWoPOgD0bbs--HngFeE.Lzzzo4mp2OmA8CyOocHBl7mJ4lwwAye4nZ2syIrWSn4
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/admin/challenges

Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3A-yVqK72LsTaXr7JFmktRDMleCleV4_CP.djdZS9YQOmUqVVl126GNM7ruIK3PZJr%2BvTBR5eUCblc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/auth/discord_cb?code=NUnqDUNeHxMt9LjAEYdpmfxHDh4buM
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AKIByBJ5PbGx1u0nrCWZinOql3u7cADtI.eXb2EuBUWcamGTzxqPOoGt7fJadfMAuUj9C0SgsEkhQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/contests/24/asd
Method	GET

Parameter	engineerman.sid
Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	https://adservice.google.com/adsid/google/si?gadsid=AORoGNRfzEOEOU6HVESnimbmzwWbmes6qJ1Dq5ge5O5Rn1CY2_x6WyhEB5AW
Method	GET
Parameter	ANID
Attack	
Evidence	AHWqTUlwsXKjPxyqeaYEwqmnj6dIH4KfHSa9VraPjmtqHOB9MnkR1h2ftHv1KBRg
Other Info	cookie:ANID
URL	https://discord.com/api/v10/oauth2/authorize?client_id=496807648289882112&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&response_type=code&scope=identify%20email
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid cookie:__sdcfduid cookie:__dcfduid cookie:__cfruid
URL	https://groups.google.com/group/zaproxy-hud
Method	GET
Parameter	NID
Attack	
Evidence	513=LkSdvfv-yebxZFLt6DEIyzIt7orj3KlavmHcULUClmr9voYHru0bcja9fZo-Av5TSE3Yxfsk8LQcDPKVJwwgr-xCcVOHe9LXmnS5Bpjx3EgruSkkhU9N4G9kBDGFivGs3xAlwpA8nCpUJZOH0kZRIHQQPGQd7gGN0AG7e6jnzmU
Other Info	cookie:NID
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/client_204?cs=1&opi=89978449
Method	GET

Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR cookie:NID
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR cookie:NID cookie:AEC
URL	https://discord.com/api/v9/auth/mfa/totp
Method	POST
Parameter	token
Attack	
Evidence	MjIyMDA1NzUwNTk4MjA1NDQw.Gi_xm1.RhIYCxoPJLDWj-nd4bOyda-74BDQXoEeqqUGLU
Other Info	json:token cookie:__Secure-recent_mfa
URL	https://discord.com/cdn-cgi/challenge-platform/h/b/jsd/r/872cb0975e860fd6
Method	POST
Parameter	cf_clearance
Attack	

Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Parameter	NID
Attack	
Evidence	513=Fkhp3GTWS2SApZ3zxO5GyFQ7dxE02zAQ_kjbuvGYHTlExnc-OurKejpw0BB7nNH5_Gx_2W9ecARSaJghihS1C2A51rA-w_bLlGlx4DLHM0nLs1uqQ63a9qWvErmub4yk1SG__CvVFpHpkdMrDgp13zF1qFOQvZ9HFPJ7kO4pzk5hRDkmXkjP8Q
Other Info	cookie:NID
URL	http://127.0.0.1:2005/
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856731.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856926.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/@brikaasdev0096
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856744.0.0.0

Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/admin
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856648.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/admin
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856752.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856659.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/admin/challenges
Method	GET
Parameter	engineerman.sid

Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856781.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/admin/contests
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/admin/contests/create
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid

URL	http://127.0.0.1:2005/api/v2/piston/runtimes
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/api/v2/piston/runtimes
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/cdn/avatars/1.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/cdn/avatars/1.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856656.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/cdn/avatars/1.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856730.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/cdn/avatars/1.png
Method	GET
Parameter	_gid

Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/cdn/avatars/1.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/cdn/avatars/2.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856744.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857325.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/challenges
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga

URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.0.1712856522.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856606.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856748.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856885.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests/24/asd
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856795.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests/disallowed_languages/24
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	

Evidence	GS1.1.1712856522.2.1.1712856829.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests/disallowed_languages/24
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AA64eAgqV86JpEBoMW4cLfGica56li11m.gX%2Fj1EIWogv6jK%2Bi%2BBLzL76cGgM5bTjW00GhJfrL9XQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856648.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/images/icon_circle_64.png

Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856656.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856731.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856887.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	engineerman.sid
Attack	

Evidence	s%3AKIByBJ5PbGx1u0nrCWZinOql3u7cADtI.eXb2EuBUWcamGTzxqPOoGt7fJadfMAuUj9C0SgsEkhQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/images/icon_circle_64.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/images/lang_icons/easy/haskell.svg
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/images/lang_icons/easy/haskell.svg
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856730.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/images/lang_icons/easy/haskell.svg
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid

URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856682.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856862.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856891.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	

Evidence	GS1.1.1712856522.2.1.1712857316.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AA64eAgqV86JpEBoMW4cLfGica56li11m.gX%2Fj1EIWogv6jK%2Bi%2BBLzL76cGgM5bTjW00GhJfrL9XQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AKIByBJ5PbGx1u0nrCWZinOql3u7cADtI.eXb2EuBUWcamGTzxqPOoGt7fJadfMAuUj9C0SgsEkhQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid

URL	http://127.0.0.1:2005/lib/bootbox/bootbox.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856552.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856654.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856891.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	_gid

Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.css.map
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856682.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856829.0.0.0
Other Info	cookie:_ga_N33Q40M7WG

URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AA64eAgqV86JpEBoMW4cLfGica56li11m.gX%2Fj1EIWogv6jK%2Bi%2BBLzL76cGgM5bTjW00GhJfrL9XQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AKIByBJ5PbGx1u0nrCWZinOql3u7cADtI.eXb2EuBUWcamGTzxqPOoGt7fJadfMAuUj9C0SgsEkhQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/bootstrap/bootstrap.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET

Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856606.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856829.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856928.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid

URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AA64eAgqV86JpEBoMW4cLfGica56li11m.gX%2Fj1EIWogv6jK%2Bi%2BBLzL76cGgM5bTjW00GhJfrL9XQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/atom-one-dark.css
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856682.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_ga_N33Q40M7WG

Attack	
Evidence	GS1.1.1712856522.2.1.1712856862.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856891.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856928.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AKIByBJ5PbGx1u0nrCWZinOql3u7cADtI.eXb2EuBUWcamGTzxqPOoGt7fJadfMAuUj9C0SgsEkhQ
Other Info	cookie:engineerman.sid

URL	http://127.0.0.1:2005/lib/highlightjs/highlight-ln.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856829.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857316.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	engineerman.sid

Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/highlightjs/highlight.pack.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856606.0.0.0
Other Info	cookie:_ga_N33Q40M7WG

URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856654.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856682.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857333.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/jquery/jquery-3.0.0.min.js
Method	GET
Parameter	engineerman.sid

Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856606.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856862.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856928.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857333.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/popper/popper.min.js

Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AKIByBJ5PbGx1u0nrCWZinOql3u7cADtI.eXb2EuBUWcamGTzxqPOoGt7fJadfMAuUj9C0SgsEkhQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/popper/popper.min.js
Method	GET
Parameter	engineerman.sid

Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856552.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/4.bundle.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid

URL	http://127.0.0.1:2005/lib/webpack/41.bundle.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856731.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/9242107df7da7c6ad3cadf3133abcd37.ttf
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/9242107df7da7c6ad3cadf3133abcd37.ttf
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856552.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/9242107df7da7c6ad3cadf3133abcd37.ttf
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/9242107df7da7c6ad3cadf3133abcd37.ttf
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/editor.worker.js
Method	GET
Parameter	_ga_N33Q40M7WG

Attack	
Evidence	GS1.1.1712856522.2.1.1712856552.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712848969921
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856648.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712848969921
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712857323608
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712857323608
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857316.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712857323608

Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857333.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712857323608
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.css?1712857323608
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856606.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	

Evidence	GS1.1.1712856522.2.1.1712856656.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856659.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856731.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712848969921
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET

Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856829.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856829510
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856862.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856884638
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967

Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856891.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856927.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712856924268
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AhhDVVWGOCLaFv0LDXmP1XF7_zC0Y11hc.FqasXCzUaX56P0rjYolranvhKQNDEQlifvZeqbnVtME
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET

Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857316.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/main.bundle.js?1712857323608
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/monaco.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0

Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856543.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856654.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712848969921
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856829510
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856829510
Method	GET

Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856829.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856829510
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AqXs9ctjXhA53PLEgbL8FqgbFYeJtKv6I.4fwvZHMS0st7ssZmXXqFy1G4b9sUAnrRC8wEbjCZ6Dc
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856884638
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856862.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712856884638
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712857323608
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712857316.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712857323608
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967

Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712857323608
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AA64eAgqV86JpEBoMW4cLfGica56li11m.gX%2Fj1EIWogv6jK%2Bi%2BBLzL76cGgM5bTjW00GhJfrL9XQ
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/react.bundle.js?1712857323608
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3AmowWqCxLsDV7b1xNj3SEZszPVhQ__O2F.3j8OJbqKLdRfVM9vAmHEn4LYW3SgQtOXy5iBPQc9hps
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856552.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856575.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET

Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/lib/webpack/ts.worker.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856544.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/balloon-white-exclamation.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/balloon-white-exclamation.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/balloon-white-exclamation.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967

Other Info	cookie:_gid
URL	http://127.0.0.1:35769/balloon-white-exclamation.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/balloon.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/break-off.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/break-off.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/break-off.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/crosshairs.png
Method	GET

Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/crosshairs.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/crosshairs.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/exclamation-red.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/exclamation-red.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/exclamation-red.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967

Other Info	cookie:_gid
URL	http://127.0.0.1:35769/exclamation-red.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/flame-grey.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/flame.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/flame.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/gear-exclamation.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/gear-exclamation.png
Method	GET

Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/gear-exclamation.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/History.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/History.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/History.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/History.js
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q

Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/latest/meta-data/
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/page-alerts-high.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/page-alerts-high.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/page-alerts-high.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/page-alerts-high.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/page-alerts-low.png
Method	GET

Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/page-alerts-low.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/page-alerts-low.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/page-alerts-low.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/plus.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/plus.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0

Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/plus.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/plus.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/radar-grey.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/radar-grey.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/radar-grey.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/radar.png
Method	GET

Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/radar.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/radar.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856606.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/radar.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/radar.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/report.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967

Other Info	cookie:_ga
URL	http://127.0.0.1:35769/report.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/report.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/report.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/script-add.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/script-add.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/script-add.png
Method	GET

Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/script-add.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/script-disabled.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/script-disabled.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/script-disabled.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/script-disabled.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q

Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/show-off.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/show-off.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/show-on.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/show-on.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/show-on.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/show-on.png
Method	GET

Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/site-alerts-high.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/site-alerts-high.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/site-alerts-high.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/site-alerts-low.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/site-alerts-medium.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967

Other Info	cookie:_ga
URL	http://127.0.0.1:35769/site-alerts-medium.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/site-alerts-medium.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/SiteAlerts.js
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/SiteAlerts.js
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/SiteAlerts.js
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/spider.png
Method	GET

Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/spider.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/spiderAjax.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/spiderAjax.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/spiderAjax.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/target-grey.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967

Other Info	cookie:_ga
URL	http://127.0.0.1:35769/target-grey.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/target-grey.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/target-grey.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/tutorial.css
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/tutorial.css
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/tutorial.css
Method	GET

Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/tutorial.css
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:35769/world.png
Method	GET
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:35769/world.png
Method	GET
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712851967.1.0.1712851967.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:35769/world.png
Method	GET
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:35769/world.png
Method	GET
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q

Other Info	cookie:engineerman.sid
URL	https://adservice.google.com/adsid/google
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://adservice.google.com/adsid/google
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://adservice.google.com/adsid/google
Method	GET
Parameter	NID
Attack	
Evidence	513=Fkhp3GTWS2SApZ3zxO5GyFQ7dxE02zAQ_kjbuvGYHTlExnc-OurKejpw0BB7nNH5_Gx_2W9ecARSaJghihS1C2A51rA-w_bLlGlx4DLHM0nLs1uqQ63a9qWvErmub4yk1SG__CvVFpHpkdMrDgp13zF1qFOQvZ9HFPJ7kO4pzk5hRDkmXkjP8Q
Other Info	cookie:NID
URL	https://adservice.google.com/adsid/google/si?gadsid=AORoGNRfzEOEOU6HVESnimbmzwWbmes6qJ1Dq5ge5O5Rn1CY2_x6WyhEB5AW
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://adservice.google.com/adsid/google/si?gadsid=AORoGNRfzEOEOU6HVESnimbmzwWbmes6qJ1Dq5ge5O5Rn1CY2_x6WyhEB5AW
Method	GET
Parameter	NID
Attack	
Evidence	513=Fkhp3GTWS2SApZ3zxO5GyFQ7dxE02zAQ_kjbuvGYHTlExnc-OurKejpw0BB7nNH5_Gx_2W9ecARSaJghihS1C2A51rA-w_bLlGlx4DLHM0nLs1uqQ63a9qWvErmub4yk1SG__CvVFpHpkdMrDgp13zF1qFOQvZ9HFPJ7kO4pzk5hRDkmXkjP8Q

Other Info	cookie:NID
URL	https://discord.com/api/v9/auth/location-metadata
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/api/v9/auth/location-metadata
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/api/v9/auth/location-metadata
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	__Secure-recent_mfa
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE3MTI4NTY1MTcsIm5iZiI6MTcxMjg1NjUxNywiZXhwIjoxNzEyODU2ODE3LCJpc3MiOiJ1cm46ZGlzY29yZC1hcGkiLCJhdWQiOiJ1cm46ZGlzY29yZC1tZmEtcmVwcm9tcHQiLCJ1c2VyIjoyMjIwMDU3NTA1OTgyMDU0NDB9.yzuDzjLLD99ef5pQkz-aXQRvnQGqWcQmpQZ7t0Fv6vh0dvD8DqVaknULicnY4dNfMqMLAYSfZEy3mQ8RxGv6ZQ

Other Info	cookie:__Secure-recent_mfa
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/api/v9/experiments
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/api/v9/experiments?with_guild_experiments=true
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email&integration_type=0
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f

Other Info	cookie:__dcfduid
URL	https://discord.com/assets/04bca5e801a9fcbfc3aa.woff2
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/04bca5e801a9fcbfc3aa.woff2
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/04bca5e801a9fcbfc3aa.woff2
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/04bca5e801a9fcbfc3aa.woff2
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/04bca5e801a9fcbfc3aa.woff2
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/07b3122d5031b91257f3.js
Method	GET

Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/07b3122d5031b91257f3.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/07b3122d5031b91257f3.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/07b3122d5031b91257f3.js
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/149536fc0fe57c89fa23.png
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/149536fc0fe57c89fa23.png
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f

Other Info	cookie:__dcfduid
URL	https://discord.com/assets/149536fc0fe57c89fa23.png
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/149536fc0fe57c89fa23.png
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/149536fc0fe57c89fa23.png
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/17764.2aa7ee221234529f6e80.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/17764.2aa7ee221234529f6e80.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/17764.2aa7ee221234529f6e80.js
Method	GET

Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/17764.2aa7ee221234529f6e80.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/200944d085aeab393864.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/26f8bedcf443fe85902f.png
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/26f8bedcf443fe85902f.png
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/26f8bedcf443fe85902f.png
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb

Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/26f8bedcf443fe85902f.png
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/26f8bedcf443fe85902f.png
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/2797.a012718ee3dfd4179128.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/3ab597cfbd4348b4d621.svg
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/43455.8c79ce3e1753b38de4a4.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/43455.8c79ce3e1753b38de4a4.js
Method	GET

Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/43455.8c79ce3e1753b38de4a4.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/43455.8c79ce3e1753b38de4a4.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/47f497e8cfdc099c8c01.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/47f497e8cfdc099c8c01.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/56a5e5a759d087feebf0.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f

Other Info	cookie:__dcfduid
URL	https://discord.com/assets/57878.f80f2ae72af75d9274b1.js
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/58661.0e645890ea50d43648f6.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/64787.359c4aba4bf61ba67cc0.js
Method	GET

Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/64787.359c4aba4bf61ba67cc0.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/64787.359c4aba4bf61ba67cc0.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/64787.359c4aba4bf61ba67cc0.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/66635.1ad04eeb540c570d5e05.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/66635.1ad04eeb540c570d5e05.js
Method	GET
Parameter	cf_clearance
Attack	

Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/67535.a3d024cb667257cc4585.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/67535.a3d024cb667257cc4585.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/67535.a3d024cb667257cc4585.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/67535.a3d024cb667257cc4585.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/67535.a3d024cb667257cc4585.js
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance

URL	https://discord.com/assets/70397.226bb847204914e85d62.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/70397.226bb847204914e85d62.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/70397.226bb847204914e85d62.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/70397.226bb847204914e85d62.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/73422.101c1055378189203ef5.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/73422.101c1055378189203ef5.js
Method	GET
Parameter	__sdcfduid

Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/75492.0148c7b424d039f78965.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/75492.0148c7b424d039f78965.js
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/85514.4384a756cb8409699d33.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/85514.4384a756cb8409699d33.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/85514.4384a756cb8409699d33.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb

Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/85514.4384a756cb8409699d33.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/86691.5616f1f9bb62628b6533.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/87dc123baf1996fe4423.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/87dc123baf1996fe4423.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/87dc123baf1996fe4423.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/90687.8573be403cf58ebc2a36.js
Method	GET

Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/98b772b4782208b1374c.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/98b772b4782208b1374c.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/99387.60d679d37e166fdc8632.css
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/99387.60d679d37e166fdc8632.css
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/99387.60d679d37e166fdc8632.css
Method	GET
Parameter	__sdcfduid
Attack	

Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/99387.60d679d37e166fdc8632.css
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/b6e61cc624d1ee35c8b4.svg
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/c6a42c9d9be5779449b4.woff2
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/c6a42c9d9be5779449b4.woff2
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/c6a42c9d9be5779449b4.woff2
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/c6a42c9d9be5779449b4.woff2

Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/c6a42c9d9be5779449b4.woff2
Method	GET
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/e16904bc61f4a8561939.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/e16904bc61f4a8561939.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/e16904bc61f4a8561939.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/e16904bc61f4a8561939.js
Method	GET
Parameter	cf_clearance

Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/assets/e66e5fa5777216466869.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/e66e5fa5777216466869.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/f7eee8828b39e32d39bc.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/f7eee8828b39e32d39bc.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/f7eee8828b39e32d39bc.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb

Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/f7eee8828b39e32d39bc.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/sentry.765b00e66783ff42fca1.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/assets/sentry.765b00e66783ff42fca1.js
Method	GET
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/assets/sentry.765b00e66783ff42fca1.js
Method	GET
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/sentry.765b00e66783ff42fca1.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/assets/shared.54491af62d8ce9108c2b.js
Method	GET

Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/assets/shared.54491af62d8ce9108c2b.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/cdn-cgi/challenge-platform/scripts/jsd/main.js
Method	GET
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/cdn-cgi/challenge-platform/scripts/jsd/main.js
Method	GET
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://play.google.com
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/async
Method	GET
Parameter	1P_JAR
Attack	

Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/async
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/async
Method	GET
Parameter	DV
Attack	
Evidence	U6Ia2BODul0TAJonGalrPPVFjcLk7Bg
Other Info	cookie:DV
URL	https://www.google.com/async
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/async/bgasy?ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449&client=firefox-b-d&yv=3&cs=0&async=_fmt:jspb
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/async/bgasy?ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449&client=firefox-b-d&yv=3&cs=0&async=_fmt:jspb
Method	GET
Parameter	NID
Attack	

Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/client_204?atyp=i&biw=1288&bih=701&dpr=1.25&ei=4SMYZoekC5OjhbIPu4WF0AE&opi=89978449
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/complete/search?q&cp=0&client=gws-wiz-serp&xssi=t&gs_pcrt=2&hl=ar&authuser=0&psi=4SMYZoekC5OjhbIPu4WF0AE.1712858082729&dpr=1.25&nolsbt=1
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/complete/search?q=CVE-2019-8331&cp=0&client=desktop-gws-wiz-on-focus-serp&xssi=t&gs_pcrt=3&hl=ar&authuser=0&pq=CVE-2019-8331&psi=4SMYZoekC5OjhbIPu4WF0AE.1712858082729&dpr=1.25&ofp=EAEYqZLkpqTji5I9GN6n1M-yoebygAEYs93WxLTzmLTWARj9-PTH_4D3-ZYBGNeU3Z-I49m6HDKXAQoXChVjdmUtMjAxOS04MzMxIGV4cGxvaXQKEAoOQ1ZFLTIwMTktMTEzNTgKEAoOQ1ZFLTIwMjEtNDExODQKEAoOQ1ZFLTIwMjAtMjMwNjQKDwoNQ1ZFLTIwMTUtOTI1MQoQCg5DVkUtMjAyMC0xMTAyMwoQCg5DVkUgMjAxNiAxMDczNQoPCg1DVkUtMjAxNi03MTAzEEc
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc

Other Info	cookie:NID
URL	https://www.google.com/compressiontest
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/compressiontest/gzip.html
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=4SMYZoekC5OjhbIPu4WF0AE&zx=1712858084124&opi=89978449
Method	GET
Parameter	DV
Attack	
Evidence	U6Ia2BODul0TAJonGalrPPVFjcLk7Bg

Other Info	cookie:DV
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=kMFpHd,sy8q,bm51tf?xjs=s3
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=kMFpHd,sy8q,bm51tf?xjs=s3
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=kMFpHd,sy8q,bm51tf?xjs=s3
Method	GET

Parameter	NID
Attack	
Evidence	513=hTstlQ33Fh8dPB3QwzYUZjfB8kV-wIg8CPlQIH_Yf6ONzyEVzBQZxROCduIYbug1pOwuQpMbdjCfeXJvp9sM4ZGlxdme2G-wfbLMmtClb2O5ntSDXPev0tCEgVtFYn_oqU_KdGvGE118bwjoyVtlquipiZSEGjGWG6w1HSHDYUdM80nVxnuBcWrr
Other Info	cookie:NID
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=syfa,syfb,aLUfP?xjs=s3
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=syfa,syfb,aLUfP?xjs=s3
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3
Method	GET
Parameter	1P_JAR

Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3
Method	GET
Parameter	DV
Attack	
Evidence	U6Ia2BODuI0TAJonGaIrPPVFjcLk7Bg
Other Info	cookie:DV
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=0/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/m=uKlGbf,sy1o5,sy3t9,DpX64d,sy3ta,EufiNb,syxx,P10Owf,syrd,syro,gSZvdb,sy5ok,vTw9Fc,sylv,syo9,syoa,syob,syoc,syod,DPreE,sy5uv,sy664,SC7lYd,sy2dp,sy3fd,bpec7b,sy2o7,qcH9Lc,sysr,sy31u,sy3th,YFicMc,syvd,syvf,syxa,WlNQGd,sy2go,sy2gp,nabPbb,syr3,syvc,syve,CnSW2d,syxg,syxh,syxi,syxj,syxl,syxm,sy47g,sy6sx,VD4Qme,syf7,BYwJlf,synk,synt,syny,VEbNoe,pjDTFb,sy1kx,sy2ng,sy2ns,sy2nt,KgxeNb,sy2nn,khkNpe?xjs=s3

Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:IPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAABAKp24PAQASA/d=1/ed=1/dg=2/rs=ACT90oGJPoXHBbrOWhW6jNRgkYcFY_zJjw/

	ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf,FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe,KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO,fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO,fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR

URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:MIhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:l46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4Ile:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX

	2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,msmzHf,pHXghd,qddgKe,sTsDMc,tIj4fb,xdV1C/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIIb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE

	9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PICTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohlYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:lvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:K

	UM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/k=xjs.s.ar.pkNDdyc4yhg.O/ck=xjs.s.WBX-9qbcbmE.R.F4.O/am=4AMKAQCAwKABAQAAAAAAAAAAAAAkAAAQgAAAAAlgSCAcIACsAEIAPjgEABgCAAQAEACVgGyEKAAQQDAABCCAH7-FwAAHIAAAACETUCAAIQLIAmBHAQAIAITDJAKAAw_AgAAQAIAAAME7AcgIAABwEMUCAgGwADjHwAFARCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAAAAABAKp24PAQASA/d=1/exm=SNUn3,attn,cEt90b,cdos,csi,d,dtl0hd,eHDfl,gwc,hsm,jsa,mb4ZUb,qddgKe,sTsDMc/excm=ABxRVc,AD6AIb,FmnE6b,JxE93,KYXthe,KiXlnd,NsEUGe,Oa7Qpb,Ok4XMd,PlCTlc,PoJj8d,PvSBGf,SpjoE,TO0csb,TurKxc,U3Ovcc,Ut0TMc,VL58m,VZLyBe,WFRJOb,XHo6qe,YuNOCb,ZGLUZ,ZrXR8b,adn7N,ak946,bXyZdf,cKV22c,fNMhz,jkRPje,kCkfUb,qngJBf,rL2AR,tzTB5,xB2dQd,y25qZb,yChgtb,ypVg7e/ed=1/dg=2/ujg=1/rs=ACT90oFAqRpamfVV5xHetFrqElia9lY_Yw/ee=ALeJib:B8gLwd;AfeaP:TkrAjf;Afksuc:wMx0R;BMxAGc:E5bFse;BgS6mb:fidj5d;BjwMce:cXX2Wb;CxXAWb:YyRLvc;DM55c:imLrKe;DULqB:RKfG5c;Dkk6ge:wJqrrd;DpcR3d:zL72xf;EABSZ:MXZt9d;ESrPQc:mNTJvc;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;EnlcNd:WeHg4;Erl4fe:FloWmf;F9mqte:UoRcbe;Fmv9Nc:O1Tzwc;G0KhTb:LIaoZ;G6wU6e:hezEbd;GleZL:J1A7Od;HMDDWe:G8QUdb;HqeXPd:cmbnH;IBADCc:RYquRb;IoGlCf:b5lhvb;IsdWVc:qzxzOb;JXS8fb:Qj0suc;JbMT3:M25sS;JsbNhc:Xd8iUd;KOxcK:OZqGte;KQzWid:ZMKkN;KcokUb:KiuZBf;KeeMUb:HiPxjc;KpRAue:Tia57b;LBgRLc:XVMNvd;LEikZe:byfTOb,lsjVmc;LsNahb:ucGLNb;Me32dd:MEeYgc;NPKaK:PVlQOd;NSEoX:lazG7b;Np8Qkd:Dpx6qc;Nyt6ic:jn2sGd;OgagBe:cNTe0;Oj465e:KG2eXe;OohIYe:mpEAQb;Pjplud:EEDORb,PoEs9b;PqHfGe:im2cZe;Q1Ow7b:x5CSu;Q6C5kf:pfdZCe;QGR0gd:Mlhmy;R2kc8b:ALJqWb;R4IIlb:QWfeKf;R9Ulx:CR7Ufe;RDNBlf:zPRCJb;SLtqO:Kh1xYe;SMDL4c:fTfGO;SNUn3:ZwDk9d,x8cHvb;ShpF6e:N0pvGc;TxfV6d:YORN0b;U96pRd:FsR04;UDrY1c:eps46d;UVmjEd:EesRsb;UyG7Kb:wQd0G;V2HTTe:RolTY;VGRfx:VFqbr;VN6jIc:ddQyuf;VOcgDe:YquhTb;VsAqSb:PGf2Re;VxQ32b:k0XsBb;WCEKNd:I46Hvd;WDGyFe:jcVOxd;Wfmdue:g3MJlb;XUezZ:sa7lqb;YV5bee:IvPZ6d;YkQtAf:rx8ur;ZMvdv:PHFPjb;ZWEUA:afR4Cf;a56pNe:JEfCwb;aAJE9c:WHW6Ef;aZ61od:arTwJ;bDXwRe:UsyOtc;bFZ6gf:RsDQqe;bcPXSc:gSZLJb;cEt90b:ws9Tlc;cFTWae:gT8qnd;coJ8e:KvoW8;dIoSBb:ZgGg9b;dLlj2:Qqt3Gf;daB6be:lMxGPd;dtl0hd:lLQWFe;eBAeSb:Ck63tb;eBZ5Nd:VruDBd;eHDfl:ofjVkb;eO3lse:nFClrf;fWLTFc:TVBJbf;g8nkx:U4MzKc;gaub4:TN6bMe;gtVSi:ekUOYd;h3MYod:cEt90b;hK67qb:QWEO5b;heHB1:sFczq;hjRo6e:F62sG;hsLsYc:Vl118;iFQyKf:QIhFr,vfuNJf;imqimf:jKGL2e;io8t5d:sgY6Zb;jY0zg:Q6tNgc;k2Qxcb:XY51pe;kCQyJ:ueyPK;kMFpHd:OTA3Ae;kbAm9d:MkHyGd;lkq0A:JyBE3e;nAFL3:NTMZac,s39S4;oGtAuc:sOXFj;oSUNyd:fTfGO;oUlnpc:RagDlc;okUaUd:wItadb;p2tIDb:tp1Cx;pKJiXd:VCenhc;pNsl2d:j9Yuyc;pXdRYb:JKoKVe;pj82le:mg5CW;qGV2uc:HHi04c;qZx2Fc:j0xrE;qaS3gd:yiLg6e;qavrXe:zQzcXe;qddgKe:d7YSfd,x4FYXe;rQSrae:C6D5Fc;sP4Vbe:VwDzFe;sTsDMc:kHVSUb;tH4IIe:Ymry6;tosKvd:ZCqP3;trZL0b:qY8PFe;uY49fb:COQbmf;uknmt:GkPrzb;uuQkY:u2V3ud;vGrMZ:lPJJ0c;vfVwPd:lcrkwe;w3bZCb:ZPGaIb;w4rSdf:XKiZ9;w9w86d:dt4g2b;wQlYve:aLUfP;wR5FRb:TtcOte;wV5Pjc:L8KGxe;whEZac:F4AmNb;xBbsrc:NEW1Qc;xbe2wc:wbTLEd;yGxLoc:FmAr0c;yxTchf:KUM7Z;z97YGf:oug9te;zOsCQe:Ko78Df;zaIgPb:Qtpxbd/m=Eox39d,GElbSc,HYSCof,IlbVv,KHourd,msmzHf,pHXghd,tlj4fb,xdV1C?xjs=s1
Method	GET
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR

URL	https://www.google.com/xjs/_/js/md=3/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA
Method	GET
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/xjs/_/js/md=3/k=xjs.s.ar.pkNDdyc4yhg.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAAkgSAAAIACAAAIAAAAAABgCAAQAEAAVgGyECAAQQDAABCCAH7-FwAAAIAAAAAETAAAAIALAAgBEAQAAAIAAAAKAAAAAAAAAAAAAAAME6AcAAAAAAAAAAAAAwADBDwABABCAA0IAAAIAAADIA_A8MByksAAAAAAAAAAAAAAAApggmAPSHxAABAAAAAAAAAAAABAKp24PAQASA
Method	GET
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	engineerman.sid

Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	http://127.0.0.1:2005/contests/submit
Method	POST
Parameter	_ga
Attack	
Evidence	GA1.1.1475577130.1712851967
Other Info	cookie:_ga
URL	http://127.0.0.1:2005/contests/submit
Method	POST
Parameter	_ga_N33Q40M7WG
Attack	
Evidence	GS1.1.1712856522.2.1.1712856795.0.0.0
Other Info	cookie:_ga_N33Q40M7WG
URL	http://127.0.0.1:2005/contests/submit
Method	POST
Parameter	_gid
Attack	
Evidence	GA1.1.629965141.1712851967
Other Info	cookie:_gid
URL	http://127.0.0.1:2005/contests/submit
Method	POST
Parameter	engineerman.sid
Attack	
Evidence	s%3ADB9QBuRSBVCFdX-vwGZgBljfrFHTHpxM.VmgC6Yk80wN5MytsCVS1XH3MpRZugGo78tsCejOoI6Q
Other Info	cookie:engineerman.sid
URL	https://discord.com/api/v9/auth/login
Method	POST
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid

URL	https://discord.com/api/v9/auth/login
Method	POST
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/api/v9/auth/mfa/totp
Method	POST
Parameter	token
Attack	
Evidence	MjIyMDA1NzUwNTk4MjA1NDQw.Gi_xm1.RhIYCxoPJLDWj-nd4bOyda-74BDQXoEeqqUGLU
Other Info	json:token
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	__dcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid

URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	__Secure-recent_mfa
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE3MTI4NTY1MTcsIm5iZiI6MTcxMjg1NjUxNywiZXhwIjoxNzEyODU2ODE3LCJpc3MiOiJ1cm46ZGlzY29yZC1hcGkiLCJhdWQiOiJ1cm46ZGlzY29yZC1tZmEtcmVwcm9tcHQiLCJ1c2VyIjoyMjIwMDU3NTA1OTgyMDU0NDB9.yzuDzjLLD99ef5pQkz-aXQRvnQGqWcQmpQZ7t0Fv6vh0dvD8DqVaknULicnY4dNfMqMLAYSfZEy3mQ8RxGv6ZQ
Other Info	cookie:__Secure-recent_mfa
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/api/v9/oauth2/authorize?client_id=496807648289882112&response_type=code&redirect_uri=http%3A%2F%2F127.0.0.1%3A2005%2Fauth%2Fdiscord_cb&scope=identify%20email
Method	POST
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://discord.com/api/v9/science
Method	POST
Parameter	__cfruid
Attack	
Evidence	8bdff5938a1da035174fe9e2f807b3637386350f-1712856472
Other Info	cookie:__cfruid
URL	https://discord.com/api/v9/science
Method	POST
Parameter	__dcfduid

Attack	
Evidence	d3372302f82811ee9e1db294636f060f
Other Info	cookie:__dcfduid
URL	https://discord.com/api/v9/science
Method	POST
Parameter	__sdcfduid
Attack	
Evidence	d3372302f82811ee9e1db294636f060fd3cd45d9fcb054e73d10a95a86842d323c11ce5a0aa29f47bd148f2ed80a3ceb
Other Info	cookie:__sdcfduid
URL	https://discord.com/api/v9/science
Method	POST
Parameter	__Secure-recent_mfa
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE3MTI4NTY1MTcsIm5iZiI6MTcxMjg1NjUxNywiZXhwIjoxNzEyODU2ODE3LCJpc3MiOiJ1cm46ZGlzY29yZC1hcGkiLCJhdWQiOiJ1cm46ZGlzY29yZC1tZmEtcmVwcm9tcHQiLCJ1c2VyIjoyMjIwMDU3NTA1OTgyMDU0NDB9.yzuDzjLLD99ef5pQkz-aXQRvnQGqWcQmpQZ7t0Fv6vh0dvD8DqVaknULicnY4dNfMqMLAYSfZEy3mQ8RxGv6ZQ
Other Info	cookie:__Secure-recent_mfa
URL	https://discord.com/api/v9/science
Method	POST
Parameter	_cfuvid
Attack	
Evidence	j6SthQwIl_.sygWC3RvE4aU6MhUNnPiKx.fQNGGX74g-1712856472157-0.0.1.1-604800000
Other Info	cookie:_cfuvid
URL	https://discord.com/api/v9/science
Method	POST
Parameter	cf_clearance
Attack	
Evidence	LjcX5wAWunM4ey4TPyou1_ZuHxeDQur3UovhKHdj7Kg-1712856479-1.0.1.1-D6gs2PlvChfdNfvZmMRgUUFokVqzbrCglsBxQqTpFf3vxxVC4I9_.5Gbd4LAAh6a2Elzd6OdVyBRjyCDk3PfbQ
Other Info	cookie:cf_clearance
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.

	876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/gen_204?atyp=csi&ei=4SMYZoekC5OjhbIPu4WF0AE&s=web&t=all&frtp=330&imn=18&ima=1&imad=0&imac=4&wh=701&aft=1&aftp=701&adh=tv.6&ime=0&imex=0&imeh=1&imeha=0&imehb=0&imea=0&imeb=0&imel=0&imed=0&scp=0&fld=1247&hp=&sys=hc.12&p=bs.false&rt=hst.820,sct.853,frts.854,prt.888,xjsls.1129,dcl.1293,frvt.1491,afti.1491,afts.877,aft.1491,aftqf.1492,xjses.1763,xjsee.1797,xjs.1797,lcp.885,fcp.876,wsrt.10,cst.0,dnst.0,rqst.805,rspt.804,sslt.0,rqstt.9,unt.0,cstt.8,dit.1301&zx=1712858082689&opi=89978449
Method	POST
Parameter	NID
Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0Ix0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,

	969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,

	1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	ANID
Attack	
Evidence	AHWqTUlwsXKjPxyqeaYEwqmnj6dIH4KfHSa9VraPjmtqHOB9MnkR1h2ftHv1KBRg
Other Info	cookie:ANID
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	DV
Attack	
Evidence	U6Ia2BODul0TAJonGaIrPPVFjcLk7Bg
Other Info	cookie:DV
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&ct=slh&v=t1&im=M&m=HV&pv=0.6033994040008019&me=1:1712858081765,V,0,0,1288,701:0,B,2199:0,N,1,4SMYZoekC5OjhbIPu4WF0AE:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,58,88,1120,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,

	1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:954,x:27,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:16,T:0,R,1,9,1090,36,92,35:0,R,1,CAgQAA,137,88,1041,47:0,R,1,CAgQAQ,508,88,670,47:0,R,1,CA0QAA,1137,88,41,47:0,R,1,CA0QAQ,1137,104,41,30:0,R,1,CAwQAA,1065,90,70,42:0,R,1,CAwQAQ,1065,90,70,42:0,R,1,CAsQAA,1020,90,43,42:0,R,1,CAsQAQ,1020,90,43,42:0,R,1,CAoQAA,969,90,49,42:0,R,1,CAoQAQ,969,90,49,42:0,R,1,CAkQAA,922,90,45,42:0,R,1,CAkQAQ,922,90,45,42:0,R,1,CAQQDQ,526,196,652,1526:0,R,1,CBsQAA,578,196,600,123:0,R,1,CBwQAA,578,349,600,123:0,R,1,CB8QAA,578,502,600,123:0,R,1,CCEQAA,578,655,600,123:3195,e,B&zx=1712858085958&opi=89978449
Method	POST
Parameter	NID
Attack	
Evidence	513=Fkhp3GTWS2SApZ3zxO5GyFQ7dxE02zAQ_kjbuvGYHTlExnc-OurKejpw0BB7nNH5_Gx_2W9ecARSaJghihS1C2A51rA-w_bLlGlx4DLHM0nLs1uqQ63a9qWvErmub4yk1SG__CvVFpHpkdMrDgp13zF1qFOQvZ9HFPJ7kO4pzk5hRDkmXkjP8Q
Other Info	cookie:NID
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449
Method	POST
Parameter	1P_JAR
Attack	
Evidence	2024-04-11-17
Other Info	cookie:1P_JAR
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449
Method	POST
Parameter	AEC
Attack	
Evidence	AQTF6HwJQy3IAn945KtHWzPSWEpr_Pj71pxItuVCwgdhlpA8LNj8FKbTkg
Other Info	cookie:AEC
URL	https://www.google.com/gen_204?atyp=i&ei=4SMYZoekC5OjhbIPu4WF0AE&dt19=2&zx=1712858083621&opi=89978449
Method	POST
Parameter	NID

Attack	
Evidence	513=Fq8CMcOuFc2aV8KO9Qj6hQvyRK0lx0rhDTmY94pOTeZWrFmoQ9PG8doIxQtSuvnD1AekUaX4pWfxTWSe0JiTPoPF0ZGrpcYZWgiwapsvnpGw8bWrA9ngBRI9WEXONQSUGj2Vi3BbFqydQegZSSxgNZTG2Lf-6Dkzcv8dFlomsbc
Other Info	cookie:NID
Instances	475
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://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/auth/discord?r=/
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/cdn/avatars
Method	GET
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/config/database.yml

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:2005/config/database.yml
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/contests
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/images
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lfm.php
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/bootbox
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/bootstrap
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/highlightjs
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/jquery
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/popper
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/lib/webpack
Method	GET
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/snippets

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:2005/snippets
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ActiveScan
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AjaxSpider
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Alerts
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/AttackMode
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	GET
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/History

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/History
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Intro
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Resend
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Show
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Spider
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/ToolConfig
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Upgrade
Method	GET
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Warning

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/Warning
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets

Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent

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://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
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://127.0.0.1:35769/WebSockets
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/admin/contests/update/24
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:2005/api/v2/piston/execute
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/AlertNotifications
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent

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://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Break
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent

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://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Comments
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Enable
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Frames
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/History
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/PageAlerts
Method	POST
Parameter	Header User-Agent

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope

Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent

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://127.0.0.1:35769/Scope
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show

Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent

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://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Show
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/SiteAlerts
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
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://127.0.0.1:35769/Sites
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	624
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**

Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	client
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: client=firefox-b-d The user-controlled value was: firefox-b-d
URL	https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331
Method	GET
Parameter	q
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://www.google.com/search?client=firefox-b-d&q=CVE-2019-8331 appears to include user input in: a(n) [textarea] tag [value] attribute The user input found was: q=CVE-2019-8331 The user-controlled value was: cve-2019-8331
URL	http://127.0.0.1:35769/Comments
Method	POST
Parameter	anticsrf
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:35769/Comments appears to include user input in: a(n) [input] tag [value] attribute The user input found was: anticsrf=76a526c7-3aa1-4958-ab14-6be4ec3d2a1c The user-controlled value was: 76a526c7-3aa1-4958-ab14-6be4ec3d2a1c
URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	field2
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:35769/Enable appears to include user input in: a(n) [input] tag [value] attribute The user input found was: field2=Disabled The user-controlled value was: disabled

URL	http://127.0.0.1:35769/Enable
Method	POST
Parameter	field3
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:35769/Enable appears to include user input in: a(n) [input] tag [value] attribute The user input found was: field3=Readonly The user-controlled value was: readonly
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	field2
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:35769/Show appears to include user input in: a(n) [input] tag [value] attribute The user input found was: field2=Hidden by using the 'hidden' type The user-controlled value was: hidden by using the 'hidden' type
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	field3
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:35769/Show appears to include user input in: a(n) [input] tag [value] attribute The user input found was: field3=Hidden by setting display to 'none' The user-controlled value was: hidden by setting display to 'none'
URL	http://127.0.0.1:35769/Show
Method	POST
Parameter	field4
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:35769/Show appears to include user input in: a(n) [input] tag [value] attribute The user input found was: field4=Hidden by setting visibility to 'hidden' The user-controlled value was: hidden by setting visibility to 'hidden'
Instances	8
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20

WASC Id	20
Plugin Id	10031