acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

21 October, 2020

Developer Report

Generated by Acunetix WVS Reporter (v10.5 Build 20160217)

Scan of https://www.uber.com:443/lk/en/drive/

Scan details

Scan information	
Start time	10/21/2020 2:40:35 AM
Finish time	10/21/2020 3:01:40 AM
Scan time	21 minutes, 5 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	**6**
High	0
Medium	1
Low	5
Informational	0

Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- txt => 1 file(s)

Top 10 response times

The files listed below had the slowest response times measured during the crawling process. The average response time for this site was 578.29 ms. These files could be targetted in denial of service attacks.

1. /lk/en/drive/contact, response time 1172 ms

GET /lk/en/drive/contact/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/contact/
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};
marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0.
_7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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%22:79.52180482. /lk/en/drive/how-much-drivers-make, response time 860 ms

GET /lk/en/drive/how-much-drivers-make/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/how-much-drivers-make/
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};
marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0._7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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%22:9.893. /lk/en/drive/basics, response time 859 ms

GET /lk/en/drive/basics/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/basics/
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};
marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0._7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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}%4. /lk/en/drive/delivery, response time 766 ms

GET /lk/en/drive/delivery/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/delivery
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};
marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0._7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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%22:79.5218045. /lk/en/drive/how-it-works, response time 704 ms

GET /lk/en/drive/how-it-works/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/how-it-works/
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};

marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0.
_7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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%22:6.
/lk/en/drive/driver-app, response time 610 ms

GET /lk/en/drive/driver-app/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/driver-app/
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};
marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0.
_7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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.
57. /lk/en/drive/safety, response time 610 ms

GET /lk/en/drive/safety/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.uber.com/lk/en/drive/safety/
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856};
marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM1OTYzNX0.
_7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY;
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}%

List of files with inputs

These files have at least one input (GET or POST).

- /lk/en/drive - 3 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed. (Configuration-> Scan Settings ->Scanning Options-> List of hosts allowed).

- get.uber.com
- twitter.com
- help.uber.com
- www.ubereats.com
- privacy.uber.com
- investor.uber.com
- instagram.com
- www.facebook.com
- accessibility.uber.com
- www.linkedin.com
- play.google.com
- apps.apple.com

- partners.uber.com
- www.youtube.com
- d1a3f4spazzrp4.cloudfront.net
- d3i4yxtzktqr9n.cloudfront.net
- tags.tiqcdn.com
- m.uber.com
- www.google.com

Alerts summary

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-352

Affected items	Variation
/lk/en/drive (64adbddee16dbd3ed58373c9670b7daa)	1

Cookie without HttpOnly flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	3

Cookie without Secure flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	1

Login page password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/lk/en/drive/	1

Alert details

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/lk/en/drive (64adbddee16dbd3ed58373c9670b7daa)

Details

Form name: <empty>
Form action: https://www.uber.com/lk/en/drive/
Form method: GET

Form inputs:

- firstName [Text]
- lastName [Text]
- email [Text]
- password [Password]
- contactInfo [Text]
- city [Text]
- inviterCode [Text]

Request headers

```
GET /lk/en/drive/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie:
_ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856
}; marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM
1OTYzNX0._7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY
Host: www.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/
Details
Cookie name: "uber_sites_geolocalization" Cookie domain: "www.uber.com"
Request headers
`GET / HTTP/1.1`

/
Details
Cookie name: "marketing_vistor_id" Cookie domain: "uber.com"
Request headers
`GET / HTTP/1.1`

/
Details
Cookie name: "_ua" Cookie domain: "www.uber.com"
Request headers
`GET / HTTP/1.1`

Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/
Details
Cookie name: "uber_sites_geolocalization" Cookie domain: "www.uber.com"
Request headers
`GET / HTTP/1.1`

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/lk/en/drive/

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
GET
/lk/en/drive/?city=Colombo%2c%20Sri%20Lanka&contactInfo=1&email=UDP6U548%40www.uber.com&
firstName=tyouyljg&inviterCode=94102&lastName=rjvlvtic&password=tQchPJp8 HTTP/1.1
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Referer: https://www.uber.com:443/lk/en/drive/
Host: www.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

Scanned items (coverage report)

Scanned 11 URLs. Found 1 vulnerable.

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

Vulnerabilities have been identified for this URL

9 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
city	URL encoded GET
contactInfo	URL encoded GET
email	URL encoded GET
firstName	URL encoded GET
inviterCode	URL encoded GET
lastName	URL encoded GET
password	URL encoded GET

Input scheme 2	
Input name	Input type
/lk/en/drive/	Path Fragment (suffix /)

Input scheme 3	
Input name	Input type
Host	HTTP Header

URL: https://www.uber.com/lk/en/drive/requirements/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/safety/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/driver-app/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/basics/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/delivery/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/how-much-drivers-make/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/contact/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

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

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/lk/en/drive/how-it-works/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://www.uber.com/robots.txt
No vulnerabilities have been identified for this URL
No input(s) found for this URL