acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

21 October, 2020

Developer Report

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

Scan of https://brand.uber.com:443/

Scan details

Scan information	
Start time	10/21/2020 2:07:52 AM
Finish time	10/21/2020 2:23:16 AM
Scan time	15 minutes, 23 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	**2**
High	0
Medium	0
Low	2
Informational	0

Knowledge base

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 394.55 ms. These files could be targetted in denial of service attacks.

1. /, response time 5422 ms

GET / 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: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: _ua={"session_id":"d4bbeebf-c1a8-49ac-a538-a212fb103d1d","session_time_ms":1603271274879};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImNzcmYtc2VjcmV0IjoiJEgzOkPvv71q77-977-9IHd
Q77-977-977-9blxcPDvvv70j77-9XjNcYu-_vXfIpntgOSJ9LCJpYXQiOjE2MDMyNzEyNzQsImV4cCI6MTYwMzM1NzY3NH
0.9HNFwr_iVaEljO57bZpKQcqxOY8WA-wAYUur6XxGsFY
Host: brand.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*

2. /guide, response time 2594 ms

GET /guide HTTP/1.1
Pragma: no-cache

Cache-Control: no-cache
Referer: https://brand.uber.com/
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":"d4bbeebf-c1a8-49ac-a538-a212fb103d1d","session_time_ms":1603271274879};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImNzcmYtc2VjcmV0IjoiJEgzOkPvv71q77-977-9IHd
Q77-977-977-9blxcPDvvv70j77-9XjNcYu-_vXfIpntgOSJ9LCJpYXQiOjE2MDMyNzEyNzQsImV4cCI6MTYwMzM1NzY3NH
0.9HNFwr_iVaEljO57bZpKQcqxOY8WA-wAYUur6XxGsFY
Host: brand.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*

3. /terms, response time 844 ms

GET /terms HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://brand.uber.com/
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":"d4bbeebf-c1a8-49ac-a538-a212fb103d1d","session_time_ms":1603271274879};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImNzcmYtc2VjcmV0IjoiJEgzOkPvv71q77-977-9IHd
Q77-977-977-9blxcPDvvv70j77-9XjNcYu-_vXfIpntgOSJ9LCJpYXQiOjE2MDMyNzEyNzQsImV4cCI6MTYwMzM1NzY3NH
0.9HNFwr_iVaEljO57bZpKQcqxOY8WA-wAYUur6XxGsFY
Host: brand.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*

List of files with inputs

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

- / - 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).

- medium.com
- behance.net
- privacy.uber.com
- twitter.com
- instagram.com
- dribbble.com
- brand-private.uberinternal.com
- d3i4yxtzktqr9n.cloudfront.net
- docs.google.com
- images.ctfassets.net
- videos.ctfassets.net
- t.uber.com
- www.uber.com
- drive.google.com

Alerts summary

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
/	1

Slow response time

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Partial
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: High
CWE	CWE-400

Affected items	Variation
/ (64adbddee16dbd3ed58373c9670b7daa)	1

Alert details

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: "_ua"
Cookie domain: "brand.uber.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Cookie:
_ua={"session_id":"d4bbeebf-c1a8-49ac-a538-a212fb103d1d","session_time_ms":1603271274879
};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImNzcmYtc2VjcmV0IjoiJEgzOkP
vv71q77-977-9IHdQ77-977-977-9blxcPDvvv70j77-9XjNcYu-_vXfIpntgOSJ9LCJpYXQiOjE2MDMyNzEyNzQ
sImV4cCI6MTYwMzM1NzY3NH0.9HNFwr_iVaEljO57bZpKQcqxOY8WA-wAYUur6XxGsFY
Host: brand.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Slow response time

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

Description

This page had a slow response time. This type of files can be targeted in denial of service attacks. An attacker can request this page repeatedly from multiple computers until the server becomes overloaded.

Impact

Possible denial of service.

Recommendation

Investigate if it's possible to reduce the response time for this page.

Affected items

/ (64adbddee16dbd3ed58373c9670b7daa)

Details

The response time for this page was 5422 ms while the average response time for this site is 394.55 ms

Request headers

```
GET / 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":"d4bbeebf-c1a8-49ac-a538-a212fb103d1d","session_time_ms":1603271274879
};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImNzcmYtc2VjcmV0IjoiJEgzOkP
vv71q77-977-9IHdQ77-977-977-9blxcPDvvv70j77-9XjNcYu-_vXfIpntgOSJ9LCJpYXQiOjE2MDMyNzEyNzQ
sImV4cCI6MTYwMzM1NzY3NH0.9HNFwr_iVaEljO57bZpKQcqxOY8WA-wAYUur6XxGsFY
Host: brand.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

Scanned items (coverage report)

Scanned 8 URLs. Found 1 vulnerable.

URL: https://brand.uber.com/

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/	Path Fragment

Input scheme 2	
Input name	Input type
	Path Fragment
/	Path Fragment
/	Path Fragment

Input scheme 3	
Input name	Input type
Host	HTTP Header

URL: https://brand.uber.com/faq

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://brand.uber.com/guide

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://brand.uber.com/terms

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://brand.uber.com/showcase

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://brand.uber.com/downloads

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://brand.uber.com/brand-story

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://brand.uber.com/public-downloads

No vulnerabilities have been identified for this URL

No input(s) found for this URL