acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

21 October, 2020

Developer Report

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

Scan of https://auth.uber.com:443/login/?breeze_local_zone=dca11&next_url=https%3A%2F%2Fguest.uber.com%2F&state=6QRllai_N-HtTFUDreNp_3io5ZBBozjqX2cqUNTaVYw%3D

Scan details

Scan information	
Start time	10/21/2020 3:12:23 AM
Finish time	The scan was aborted
Scan time	4 hours, 2 minutes
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	**11**
High	0
Medium	2
Low	4
Informational	5

Alerts summary

BREACH attack

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 9.1 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-310
CVE	CVE-2013-3587

Affected items	Variation
/login/session	1

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
/login (8363fac6c7655f235e9ddbc9bd46fad0)	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
/	2

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
/	2

Email address found

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: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/login	1
/login/	1
/login/session	1
/login/udimeta	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/login (bc6f7ffc5a7dc1c3d567d7f49fdddbf0)	1

Alert details

BREACH attack

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (XSS.script)

Description

This web application is potentially vulnerable to the BREACH attack.

An attacker with the ability to:

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

can leverage information leaked by compression to recover targeted parts of the plaintext.

BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) is a category of vulnerabilities and not a specific instance affecting a specific piece of software. To be vulnerable, a web application must:

- Be served from a server that uses HTTP-level compression
- Reflect user-input in HTTP response bodies
- Reflect a secret (such as a CSRF token) in HTTP response bodies

Impact

An attacker can leverage information leaked by compression to recover targeted parts of the plaintext.

Recommendation

The mitigations are ordered by effectiveness (not by their practicality - as this may differ from one application to another).

- Disabling HTTP compression
- Separating secrets from user input
- Randomizing secrets per request
- Masking secrets (effectively randomizing by XORing with a random secret per request)
- Protecting vulnerable pages with CSRF
- Length hiding (by adding random number of bytes to the responses)
- Rate-limiting the requests

References

CVE-2013-3587
BREACH attack

Affected items

/login/session

Details

This alert was issued because the following conditions were met:

- The page content is served via HTTPS
- The server is using HTTP-level compression
- URL encoded POST input addPassword was reflected into the HTTP response body.
- HTTP response body contains a secret named x-csrf-token

Request headers

```
POST /login/session HTTP/1.1
Content-Length: 3719
Content-Type: application/x-www-form-urlencoded
Referer:
https://auth.uber.com:443/login/?breeze_local_zone=dca11&next_url=https%3A%2F%2Fguest.uber.com%2F&state=6QRlIai_N-HtTFUDreNp_3io5ZBBozjqX2cqUNTaVYw%3D
```

```
(line truncated)
...K0nhA%3D%3DPrj97OuNIS2Yr1RViwlydw%3D%3D8qAraL31AS6x29b1MJQULw6OENJRJe2McDh%2FJkkJtLY%
3D;
_ua=%7B%22id%22%3A%2245f4d390-c9d6-474a-bf08-31e725d82c53%22%2C%22ts%22%3A1603275163215%
7D; _cc=ARvEsqMInSFEPHrejkm2AjxE;
udi-fingerprint=qMqquWHtavdr%2BnM7qRqb3P4xp1qENXkmBztzU8pWPh4jju3GL5xyN3mOL12dIMdlvgfF5O
NZDdCEZeHbVwmFWQ%3D%3Db3H1wKvJvlBJ4shOGrXg5lBDAVLpftIv5DDGnzwTK8k%3D;
marketing_vistor_id=bba10375-b595-421c-9d24-67361f95fa62;
_cc-x=ZGQyODkwNWUtNTNkOS00YWQyLTg2OWEtNWM4NWRkY2UyY2M2OjE2MDMyNzUxNjQ2Mzc
Host: auth.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: */*

addPassword=g00dPa%2524%2524w0rD_9782&autoSMSVerificationSupported=false&countryCode=1&e
mail=sample%40email.tst&firstName=xluhnmuh&firstPartyClientID=&in ...
```

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

/login (8363fac6c7655f235e9ddbc9bd46fad0)

Details

Form name: <empty>
Form action: https://auth.uber.com/login/
Form method: POST

Form inputs:

- textInputValue [Text]

Request headers

```
GET
/login/?breeze_local_zone=dca11&next_url=https://guest.uber.com/&state=6QRlIai_N-HtTFUDr
eNp_3io5ZBBozjqX2cqUNTaVYw%3D HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: auth.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: */*
```

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: "udi-fingerprint" Cookie domain: "uber.com"
Request headers
`GET / HTTP/1.1`

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

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

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_Dir.script)

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Email Address Disclosed on Website Can be Used for Spam

Affected items

/login

Details

Pattern found: support@jump.com
business-support@uber.com
u003Esupport@uber.com
example@ubereats.com
u002Fuber@auth.uber.com

Request headers

```
GET /login/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...izgjmRwKivu19H-kaxXMd2VpkH8rTeJGq9GNd3s21DID9kSaVPFfq5BWdb87_blBcNK88i9lYpVKf8vpb2sRN
JuxFo2om-9J5JEfSaAUNeVSnsL82kKZOw7HVASryCPusFtKEO67pfvA_j_gygu7R_FnIjMRHbw5gKqAyIs2Sfmzu
Q5ald6Gn31WIh2R7mpN_DR8GeYTUrTrCyycJ1s6MeuESrGhCf7Y8AdgYF05OcofQXU3tRlW6j9SigtNI9Fo8Jzj3
Yp-w3vklqTnweWL_IsZvVjORVgniCdCzwEhdJ9X3cOTqPBBO2FQXyk_aDv1EzMPTL7KzDF131iYrthyzw0LZxoBN
cv5aZ3LJrdmpkzdDVtaCGR4d0RPxNne4nYjR_dBrCNnbJ1J3xY0p1_oi3xNVpW5nFhaG4yaqdhQwBlLMOb.16032
75144104.1209600000.tWSXr0t_qe29eyfbib2GpqtGb3uUC6GErnsN7G57YTs
Host: auth.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: */*
```

/login/

Details

Tested on URI: /login/YZCUSwJbex.jsp

Pattern found in response: support@jump.com business-support@uber.com u003Esupport@uber.com example@ubereats.com u002Fuber@auth.uber.com

Request headers

```
GET /login/YZCUSwJbex.jsp HTTP/1.1
(line truncated)
...K0nhA%3D%3DPrj97OuNIS2Yr1RViwlydw%3D%3D8qAraL31AS6x29b1MJQULw6OENJRJe2McDh%2FJkkJtLY%
3D;
```

```
_ua=%7B%22id%22%3A%2245f4d390-c9d6-474a-bf08-31e725d82c53%22%2C%22ts%22%3A1603275163215%
7D; _cc=ARvEsqMInSFEPHrejkm2AjxE;
udi-fingerprint=qMqquWHtavdr%2BnM7qRqb3P4xp1qENXkmBztzU8pWPh4jju3GL5xyN3mOL12dIMdlvgfF5O
NZDdCEZeHbVwmFWQ%3D%3Db3H1wKvJvlBJ4shOGrXg5lBDAVLpftIv5DDGnzwTK8k%3D;
marketing_vistor_id=bba10375-b595-421c-9d24-67361f95fa62;
_cc-x=ZGQyODkwNWUtNTNkOS00YWQyLTg2OWEtNWM4NWRkY2UyY2M2OjE2MDMyNzUxNjQ2Mzc
Host: auth.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: */*
```

/login/session

Details

Pattern found: support@jump.com
business-support@uber.com
u003Esupport@uber.com
example@ubereats.com
u002Fuber@auth.uber.com

Request headers

```
GET /login/session HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://auth.uber.com/login/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...izgjmRwKivu19H-kaxXMd2VpkH8rTeJGq9GNd3s21DID9kSaVPFfq5BWdb87_blBcNK88i9lYpVKf8vpb2sRN
JuxFo2om-9J5JEfSaAUNeVSnsL82kKZOw7HVASryCPusFtKEO67pfvA_j_gygu7R_FnIjMRHbw5gKqAyIs2Sfmzu
Q5ald6Gn31WIh2R7mpN_DR8GeYTUrTrCyycJ1s6MeuESrGhCf7Y8AdgYF05OcofQXU3tRlW6j9SigtNI9Fo8Jzj3
Yp-w3vklqTnweWL_IsZvVjORVgniCdCzwEhdJ9X3cOTqPBBO2FQXyk_aDv1EzMPTL7KzDF131iYrthyzw0LZxoBN
cv5aZ3LJrdmpkzdDVtaCGR4d0RPxNne4nYjR_dBrCNnbJ1J3xY0p1_oi3xNVpW5nFhaG4yaqdhQwBlLMOb.16032
75144104.1209600000.tWSXr0t_qe29eyfbib2GpqtGb3uUC6GErnsN7G57YTs
Host: auth.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: */*
```

/login/udimeta

Details

Pattern found: support@jump.com
business-support@uber.com
u003Esupport@uber.com
example@ubereats.com
u002Fuber@auth.uber.com

Request headers

```
GET /login/udimeta HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://auth.uber.com/login/session
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...K0nhA%3D%3DPrj97OuNIS2Yr1RViwlydw%3D%3D8qAraL31AS6x29b1MJQULw6OENJRJe2McDh%2FJkkJtLY%
3D;
_ua=%7B%22id%22%3A%2245f4d390-c9d6-474a-bf08-31e725d82c53%22%2C%22ts%22%3A1603275163215%
7D; _cc=ARvEsqMInSFEPHrejkm2AjxE;
udi-fingerprint=qMqquWHtavdr%2BnM7qRqb3P4xp1qENXkmBztzU8pWPh4jju3GL5xyN3mOL12dIMdlvgfF5O
NZDdCEZeHbVwmFWQ%3D%3Db3H1wKvJvlBJ4shOGrXg5lBDAVLpftIv5DDGnzwTK8k%3D;
marketing_vistor_id=bba10375-b595-421c-9d24-67361f95fa62;
```

```
_cc-x=ZGQyODkwNWUtNTNkOS00YWQyLTg2OWEtNWM4NWRkY2UyY2M2OjE2MDMyNzUxNjQ2Mzc
Host: auth.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: */*
```

Password type input with auto-complete enabled

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

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/login (bc6f7ffc5a7dc1c3d567d7f49fdddbf0)

Details

Password type input named addPassword from form with ID answerForm with action /login/session has autocomplete enabled.

Request headers

```
GET /login/?next_url=https://guest.uber.com/&source=auth&uber_client_name=riderSignUp
HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer:
https://auth.uber.com/login/?breeze_local_zone=dca11&next_url=https://guest.uber.com/&st
ate=6QRlIai_N-HtTFUDreNp_3io5ZBBozjqX2cqUNTaVYw%3D
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...izgjmRwKivu19H-kaxXMd2VpkH8rTeJGq9GNd3s21DID9kSaVPFfq5BWdb87_blBcNK88i9lYpVKf8vpb2sRN
JuxFo2om-9J5JEfSaAUNeVSnsL82kKZOw7HVASryCPusFtKEO67pfvA_j_gygu7R_FnIjMRHbw5gKqAyIs2Sfmzu
Q5ald6Gn31WIh2R7mpN_DR8GeYTUrTrCyycJ1s6MeuESrGhCf7Y8AdgYF05OcofQXU3tRlW6j9SigtNI9Fo8Jzj3
Yp-w3vklqTnweWL_IsZvVjORVgniCdCzwEhdJ9X3cOTqPBBO2FQXyk_aDv1EzMPTL7KzDF131iYrthyzw0LZxoBN
cv5aZ3LJrdmpkzdDVtaCGR4d0RPxNne4nYjR_dBrCNnbJ1J3xY0p1_oi3xNVpW5nFhaG4yaqdhQwBlLMOb.16032
75144104.1209600000.tWSXr0t_qe29eyfbib2GpqtGb3uUC6GErnsN7G57YTs
Host: auth.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: */*
```

Scanned items (coverage report)

Scanned 3 URLs. Found 3 vulnerable.

URL: https://auth.uber.com/login/

Vulnerabilities have been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
breeze_local_zone	URL encoded GET
next_url	URL encoded GET
state	URL encoded GET

Input scheme 2	
Input name	Input type
textInputValue	URL encoded POST

Input scheme 3	
Input name	Input type
next_url	URL encoded GET
source	URL encoded GET
uber_client_name	URL encoded GET

Input scheme 4	
Input name	Input type
Host	HTTP Header

URL: https://auth.uber.com/login/session

Vulnerabilities have been identified for this URL

58 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
addPassword	URL encoded POST
autoSMSVerificationSupported	URL encoded POST
countryCode	URL encoded POST
email	URL encoded POST
firstName	URL encoded POST
firstPartyClientID	URL encoded POST
inAuthSessionID	URL encoded POST
lastName	URL encoded POST
meta	URL encoded POST
nextURL	URL encoded POST
phoneNumber	URL encoded POST
promoCode	URL encoded POST
promotionValueString	URL encoded POST
sess	URL encoded POST
type	URL encoded POST
uberClientName	URL encoded POST
x-csrf-token	URL encoded POST

Input scheme 2	
Input name	Input type
textInputValue	URL encoded POST

Input scheme 3	
Input name	Input type
addPassword	JSON
autoSMSVerificationSupported	JSON
countryCode	JSON
email	JSON
firstName	JSON
lastName	JSON
nextURL	JSON
phoneNumber	JSON
promoCode	JSON
sess	JSON
type	JSON
uberClientName	JSON
x-csrf-token	JSON

Input scheme 4	
Input name	Input type
addPassword	JSON
autoSMSVerificationSupported	JSON
countryCode	JSON
nextURL	JSON
phoneNumber	JSON
sess	JSON
type	JSON
uberClientName	JSON
x-csrf-token	JSON

Input scheme 5	
Input name	Input type
addPassword	URL encoded POST
autoSMSVerificationSupported	URL encoded POST
countryCode	URL encoded POST
email	URL encoded POST
firstName	URL encoded POST
firstPartyClientID	URL encoded POST
g-recaptcha-response	URL encoded POST
inAuthSessionID	URL encoded POST
lastName	URL encoded POST
meta	URL encoded POST
nextURL	URL encoded POST
phoneNumber	URL encoded POST
promoCode	URL encoded POST
promotionValueString	URL encoded POST
sess	URL encoded POST
type	URL encoded POST
uberClientName	URL encoded POST
x-csrf-token	URL encoded POST

URL: https://auth.uber.com/login/udimeta

Vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

meta	JSON