WEB APPLICATION SECURITY

Acunetix Website Audit

21 October, 2020

Developer Report

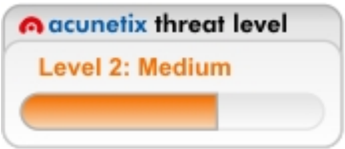
Generated by Acunetix WVS Reporter (v10.5 Build 20160217)

Scan of https://movement.uber.com:443/?lang=en-US

Scan details

Scan information	
Start time	10/21/2020 8:56:20 AM
Finish time	10/21/2020 9:01:38 AM
Scan time	5 minutes, 17 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	**3**
High	0
Medium	1
Low	2
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 452.00 ms. These files could be targetted in denial of service attacks.

1. /, response time 547 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":"30bd05ce-7d5b-4b84-856b-4c11d9b264e2","session_time_ms":1603295782035};
cookieSession={"rateLimitingID":"fce3f120-5508-4853-87f9-ec5dff3f0b38"};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyOTU3ODIsImV4cCI6MTYwMzM4MjE4Mn0.Y
ArY08cCwNtIN_V2wmbduvF86nyp6UnbntyX0un6mWQ
Host: movement.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).

- / - 2 inputs

Alerts summary

URL redirection

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 0 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-601

Affected items	Variation
Web Server	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
/	1

OPTIONS method is enabled

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
Web Server	1

Alert details

URL redirection

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Open_Redirect.script)

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

[HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics]()
[URL Redirection Security Vulnerability]()

Affected items

Web Server

Details

URI was set to //vulnweb.com.

Request headers

```
GET //vulnweb.com HTTP/1.1
Host: movement.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: "_ua"
Cookie domain: "movement.uber.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie:
_ua={"session_id":"30bd05ce-7d5b-4b84-856b-4c11d9b264e2","session_time_ms":1603295782035
}; cookieSession={"rateLimitingID":"fce3f120-5508-4853-87f9-ec5dff3f0b38"};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyOTU3ODIsImV4cCI6MTYwMzM
4MjE4Mn0.YArY08cCwNtIN_V2wmbduvF86nyp6UnbntyX0un6mWQ
Host: movement.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: */*
```

OPTIONS method is enabled

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

Description

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact

The OPTIONS method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

It's recommended to disable OPTIONS Method on the web server.

References

[Testing for HTTP Methods and XST (OWASP-CM-008)]()

Affected items

Web Server

Details

Methods allowed: GET,HEAD

Request headers

```
OPTIONS / HTTP/1.1
Host: movement.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 2 URLs. Found 1 vulnerable.

URL: https://movement.uber.com/
Vulnerabilities have been identified for this URL
2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
lang	URL encoded GET

Input scheme 2	
Input name	Input type
Host	HTTP Header

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