McDonald's Wi-Fi Login System by BT Italia S.p.A.

Multiple Vulnerabilities Report

VOIDSEC

Summary

INTRODUCTION

The McDonald's affair is a typical case of bad programming and conduct of networks security.

Analyzing the login portal for Wi-Fi system hosts we have identified an error, relatively banal, in the user account double-factored authentication generation process. It was possible register fictitious accounts jumping the obliged passage of identity check with the reception of a SMS; through analyzing the data traffic we could also recover the needed information for the registration automatism via bot.

This vulnerability allowed using the McDonald's network as a shield and proxy not only for surfing anonymously the net but also for attacking other system in total security.

Besides on the public network we have identified the presence of some backend services as a private VPN, the Wi-Fi management system and the POS (bancomat and credit cards payments gateway).

VULNERABILITIES LIST

- Non persistent XSS
- Captcha bypass
- Login bypass
- McDonald's VPN login bruteforce

VULNERABILITIES DESCRIPTION

The vulnerabilities exploited, excluding the VPN login bruteforce, are present in every Italian McDonald's with public Wi-Fi systems.

XSS

Cross-site scripting not persistent in some parameters of host's login Wi-Fi system URL: that allows the execution of a client side code for actuating a variegated whole series of attacks, for example:

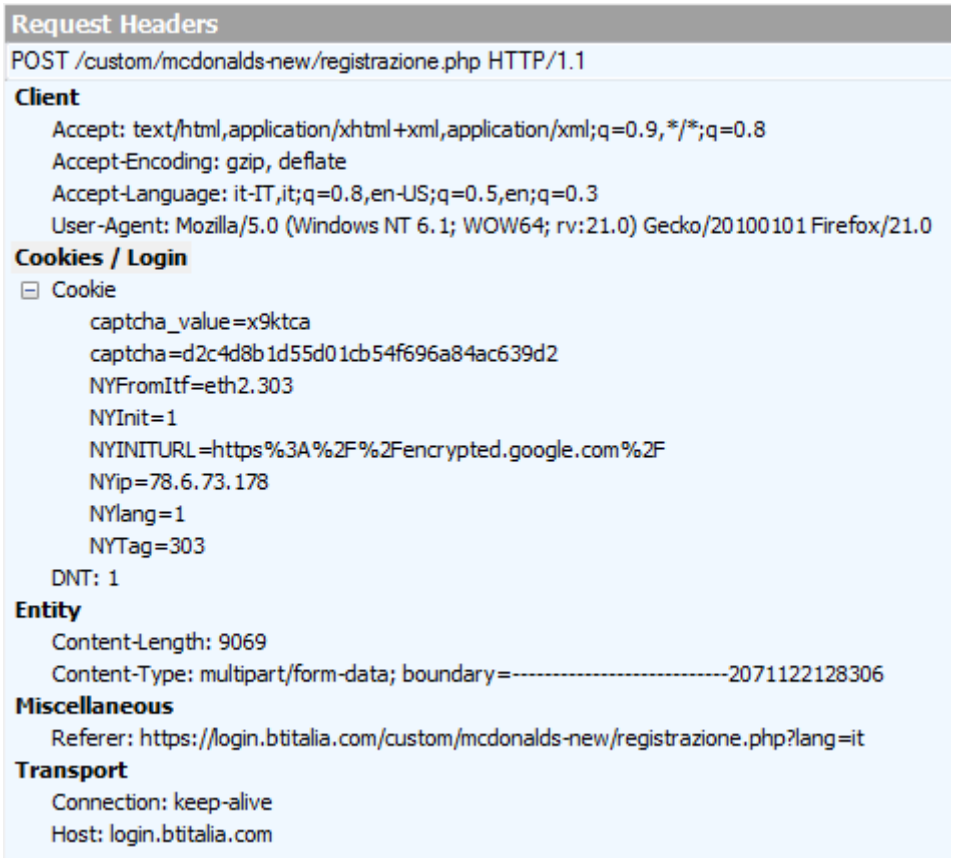
- Gathering, manipulation and redirecting of confidential information
- Data visualization and editing inside servers
- Web dynamic conduct change

In the last case is possible to inject HTML code, putting a "deface" in the home page, a redirect or a phising attempt.

CAPTCHA

Observing the client side requests and the answers given by the server is shown that the captcha solution is passed uncoded to the client via cookies, making useless a manual intervention; any bot or automatized software can get back the value from the cookie and then register with success innumerable accounts.

In detail, among URL cookies (registrazione.php) there's a captcha value field with an alphanumerical value correspondent to the image solution shown in the registration page.



LOGIN

This vulnerability has to be considered the most important because it allows any unidentified user to register with fictitious data and then to use the Wi-Fi connection for browsing anonymously and/or to use the hotspot as a proxy for attacking other infrastructures.

After the registration every user of the service is identified by the personal data given and the mobile phone telephone number used. Normally even if an ill-mentioned gives fictitious personal data the traceability would be granted by the phone number furnished; as shown below, the authentication password sent by SMS is generated by the client, making impossible the user identification in case of false telephone number.

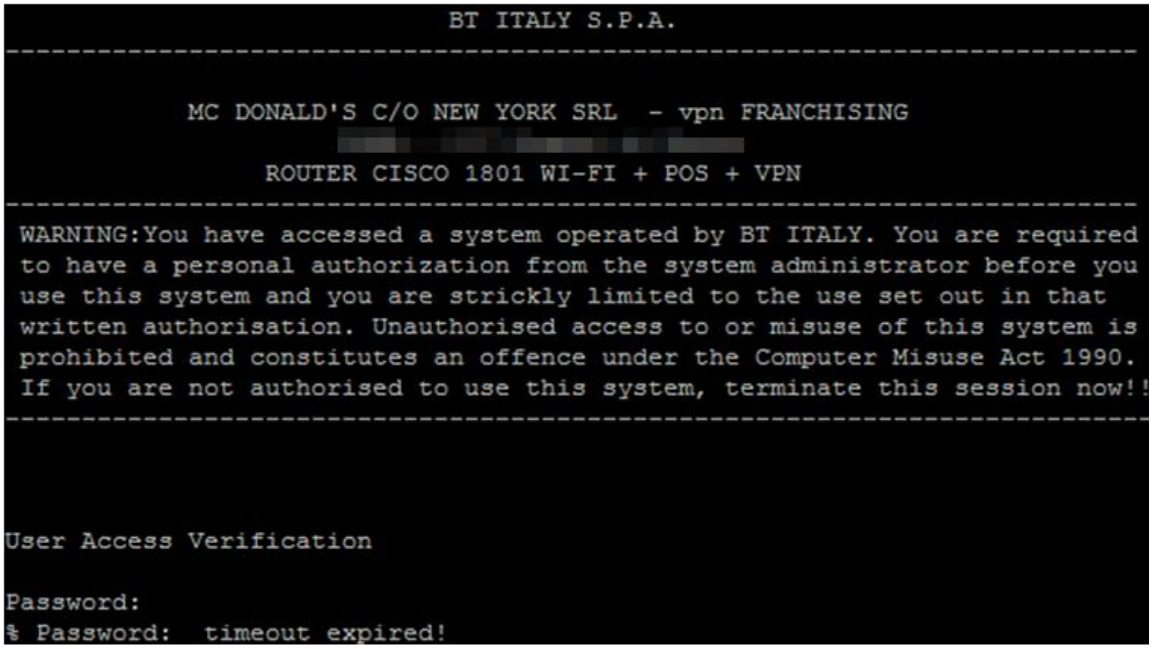
Fictitious POST DATA analysis:

Chiave	Valore
captcha	x9ktca
Consenso1	NO
Consenso2	NO
Consenso3	NO
email	mail@gmail.com
FirstName	Nome
Info1	YES
lang	1
Language	it
LastName	Cognome
operazione	
password	1Cccc11c
PhoneNumber1	3333333333
PrefixPhoneNumber1	+39
textarea	Art. 13 D.Lgs. n. 196 del 30 giugno 2003.
username	MCD_003_Utente
x	63
y	14

From that is possible to get username and password, respectively *MCD_003_Utente* and *1Cccc11c*.

VPN

On the guest's accessible network we have found, thanks to what we think it might be an incorrect configuration, an host that allowed the access to the inside VPN, to Wi-Fi and to POS.



Our ethics has prevented us from "forcing" the login system, but is important to signal how, with a bruteforce attack, is possible to try to bypass this protection.

FIX

XSS

Validate and filter further the parameters in input that can be manipulated by the user.

The most safe method for a programmer is to use one of the functions that permit the HTML characters escape putted in a string. These functions are: htmlspecialchars(), htmlentities(), strip_tags.

CAPTCHA

Never give back the captcha uncoded value. Usually for every image there's the hash of its value in the database so is possible to receive in input the user value, to run the hash and then confront it with the one memorized in the database for the authentication.

LOGIN

Generate the password and the username, for authenticating an host on the net, server side only and then send everything to the phone number acquired in input so that the user is traceable and identifiable.

VPN

If the network type allows that, insert the host with VPN access in a subnet not accessible by McDonald's guests.

CONCLUSIONS

Considering the web architecture we have “met”, compromise the back-end would had have as a result the access to the principal trade gateway of web data; thus, surely it would be impossible to steal the surfing data of McDonald’s hosts and VPN transit data.

Given the presence on the network of the POS payment system, someone might think to attack this service for stealing money; for doing some evaluation it would be necessary know the net structure; anyway we think that the attack is not very likely because the structure of POS. We have notice that recently the malware development for attacking this kind of structure is increasing. We specify that our ethic doesn’t allows us to violate and, consequently, to directly attack this system.

Quantifying the risk for the company, it would be possible to steal surfing data, potentially recover host’s registration data, redirect the web traffic on another system and eventually compromise host’s computers and web devices.

Contacting McDonald’s was easier than we had expected, because we hadn’t a contact with a competent technician. We had simply informed the presence of a vulnerability, and we’ve been – promptly – contacted by an operator, very ready to dialogue, with whom we started a collaboration.

General information

Reporter	VoidSec Security Team
Authors	Paolo Stagno, Luca Poletti
Contact	08-08-13
Vendor Response	09-08-13
Last Vendor reply	29-08-13 *
Date of public disclosure	24-11-13

* Vendor has become inactive after this date and is not responding to two successive contacts.

Common Vulnerability Scoring System 2.0 (CVSS)

Parameter	Value
CVSS Base Score	3.3
CVSS Temporal Score	3.3
CVSS Environmental Score	3.3
Overall CVSS Score	**3.3**

Full CVSS v2 VECTOR:

(AV:A/AC:L/AU:N/C:N/I:N/A:P/E:H/RL:U/RC:C/CDP:N/TD:H/CR:M/IR:L/AR:M)

Additional Informations:

Guide CVSS v2

NIST Calculator

Contacts

VoidSec Security Team | security@voidsec.com | http://voidsec.com | Vulnerability Disclosure Policy