GM Servizi

Assessment di sicurezza esterno

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	21 Dicembre 2007	Emissione.

INFORMAZIONI	
Data di Emissione	21 Dicembre 2007
Versione	1.0
Tipologia Documento	Documento di Assessment
Numero Pagine	48
Redatto da	Andrea Cariola
Approvato da	Luca Filippi Gianluca Vadruccio

INDICE

1 Sintesi tecnica

Il presente documento descrive l'attività di *vulnerability assessment* sulla rete di GM Servizi. Le attività sono state eseguite dalla sede di Hacking Team con postazioni di analisi configurate opportunamente.

L'approccio utilizzato è stato di tipo *white-box*, quindi l'analisi ha avuto luogo conoscendo alcuni dettagli del sistema *target.* I controlli da eseguire in questa fase sono stati prevalentemente di tipo sistemistico, quindi lo studio ha compreso solo marginalmente l'analisi di eventuali applicazioni *web-based* rilevate, in conseguenza al tempo disponibile ed al grado di sicurezza rilevato durante la prima fase stessa.

L'attività è stata eseguita sui sistemi in esercizio: per tale motivo tutti i *test* sono stati attentamente selezionati, sia per modalità di esecuzione che per tipologia, allo scopo di non creare alcun tipo di disservizio. Non sono state utilizzate tutte quelle tipologie di attacco che avrebbero potuto compromettere il corretto funzionamento e l'integrità dei sistemi *target*.

Lo stato di sicurezza rilevato per la rete esterna GM Servizi è di buon livello.

Di seguito riportiamo l'elenco delle vulnerabilità (più o meno significative) trovate durante i test.

- E' stata riscontrata possibilità di effettuare trasferimenti di zona su un particolare server DNS del cliente
- E' stata riscontrata possibilità di utilizzare, da parte di chiunque, un DNS di GM Servizi per risolvere i nomi di altri domini Internet
- E' stata riscontrata la presenza di codice sorgente javascript di alcune pagine web
- E' stata riscontrata la possibilità di effettuare query SQL sul database di un sito web rilevato
- E' stata riscontrata una configurazione non ottimale in uno dei server web

Le debolezze riscontrate sono potenzialmente sfruttabili da qualsiasi attaccante che disponga, semplicemente, di un accesso ad Internet.
Alcune di queste hanno un impatto più significativo sulla sicurezza dell'infrastruttura testata e andrebbero sistemate il prima possibile; altre debolezze, sebbene di minor entità, possono essere eliminate in tempi meno ristretti.

La seguente tabella sintetizza quanto riscontrato, evidenziando gli impatti delle singole vulnerabilità rilevate, le capacita tecniche necessarie al loro sfruttamento, ed il livello di rischio[1] correlato alla minaccia (si noti che la vulnerabilità tra parentesi rappresenta un valore assoluto, che nel contesto di GM Servizi viene abbassato per la sua reale valenza):

N°	Categoria di vulnerabilità	Impatto	Livello di skill tecnico necessario per lo sfruttamento	Livello di rischio della vulnerabilità
V1	DNS Zone Transfer	Consente ad un attaccante il reperimento di informazioni sulla topologia dell'infrastruttura di rete del Cliente	Basso	Basso
V2	Open DNS	Consente di effettuare attacchi di tipo Denial of Service verso terze parti	Basso	Medio
V3	SQL Injection	E' possibile eseguire *query* SQL sul database dell'applicazione dal Web	Medio	Medio (Alto)
V4	Source Code Disclosure	E' possibile visualizzare il codice sorgente di alcune applicazioni web	Basso	Medio (Alto)
V5	Metodi TRACE e TRACK HTTP abilitati	E' potenzialmente possibile recuperare informazioni sensibili	Alto	Basso

Tabella 1: Sintesi delle categorie di vulnerabilità/debolezze e dei rispettivi impatti

[1] Il livello di rischio è definibile asettico in quanto si basa su considerazioni generali legate all'esperienza Hacking Team, senza alcun riscontro relativo al core business. Le informazioni presenti sono comunque necessarie per una valutazione interna da parte del cliente, strettamente legata alle relazioni con il business: solo dopo aver determinato gli impatti sul business si potrà associare un effettivo livello di rischio ad ogni vulnerabilità.

La figura seguente mostra una classificazione delle minacce in base al livello di rischio ed alla capacità tecnica necessaria per il loro sfruttamento:

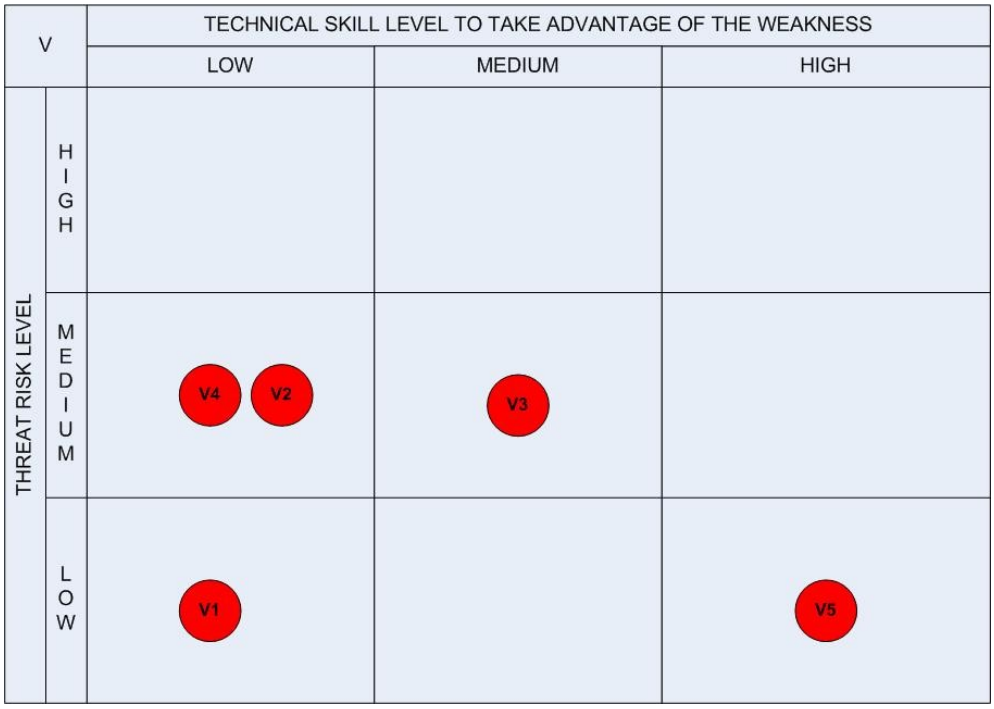

Figura 1 - Classificazione delle vulnerabilità in base al rishio ed allo skill richiesto

La tabella seguente riassume le azioni da intraprendere per la copertura dalle minacce riscontrate, e per il conseguente innalzamento del livello di sicurezza:

N°	Categoria di vulnerabilità	Soluzione proposta	Impegno richiesto per implementare la soluzione
V1	DNS Zone Transfer	Modificare la configurazione del DNS per permettere le *zone transfer* solo ai DNS che effettivamente hanno necessità di tale operazione (ad es. i secondari)	Basso
V2	Open DNS	Modificare la configurazione del DNS server per limitare la risoluzione dei nomi Internet al più alle reti interne del Cliente.	Basso
V3	SQL Injection	Per eliminare la vulnerabilità è necessaria la riscrittura del codice di interfacciamento fra le pagine WEB e il database SQL. Come ulteriore soluzione è possibile l'inserimento di un *application firewall* a monte del *web server*. Le due soluzioni non sono mutuamente esclusive.	Medio
V4	Source Code Disclosure	Impostare correttamente i permessi di accesso ai file e rimuovere i file contenenti i sorgenti delle applicazioni non più utilizzate.	Basso
V5	Metodi TRACE e TRACK HTTP abilitati	Disabilitare i metodi TRACE e TRACK modificando i file di configurazione del Web Server	Basso

Tabella 2: Sintesi della soluzione proposta e dell'impegno richiesto

La seguente figura mostra una classificazione delle minacce in base al livello di rischio, e all'*effort* necessario per prevenirle.

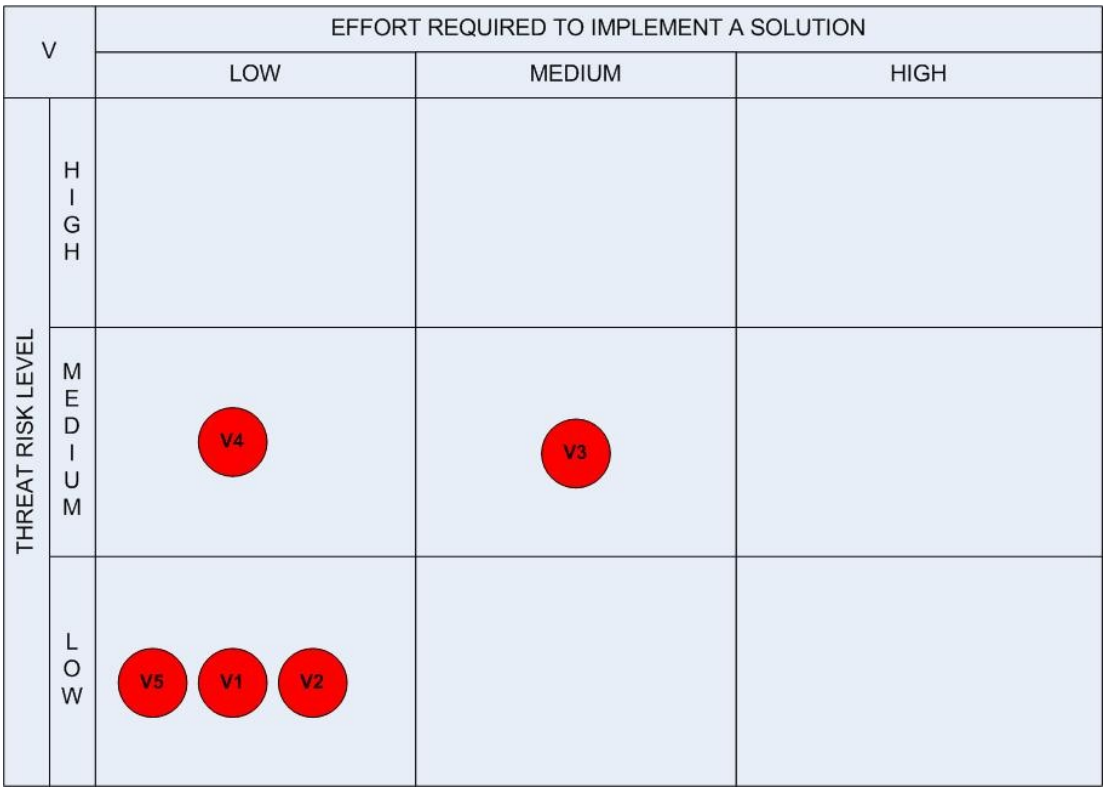

Figura 2 - Classificazione delle vulnerabilità in base al rischio e all'effort necessario per il rientro

Introduzione

1.1 Obiettivo

Le attività sono state effettuate al fine di valutare il livello di sicurezza della rete di GM Servizi, identificando le possibili minacce associate alle vulnerabilità individuate. I test di sicurezza sono stati realizzati da remoto, presso i laboratori Hacking Team di Milano.

Le attività sono state condotte seguendo un approccio tradizionale, tenendo in considerazione tutti quegli accorgimenti idonei all'effettiva esaustività del controllo di sicurezza, e senza testare invasivamente il livello di servizio offerto dal sistema di difesa esistente.

1.2 Output del lavoro

Il presente documento comprende le seguenti sezioni:

- Sintesi tecnica dei risultati
- Descrizione delle vulnerabilità riscontrate
- Analisi degli impatti delle minacce esistenti
- Piano delle contromisure a copertura delle debolezze identificate

Si ritiene inoltre opportuno elencare gli altri documenti che compongono il lavoro finale, che hanno però più significato come *"reference guide"* e che quindi sono presentati in allegato:

- Metodologia di *assessment* seguita
- *Scan reports* risultanti dai tool automatici

1.3 Vincoli e limiti del lavoro svolto

I vincoli che hanno limitato l'attività di analisi della sicurezza si possono sintetizzare nei seguenti punti:

- Non sono state effettuate attività DoS (*Denial of Service*).
- Non sono state rilasciate ai tester credenziali di accesso ai sistemi.

1.4 Perimetro del lavoro

Gli indirizzi IP che sono stati oggetti di attività sono elencati nella seguente tabella:

IP
213.204.2.49
213.204.2.50
213.204.2.58
213.204.2.59
213.204.2.60
213.204.2.61
213.204.2.62
213.204.2.98
213.204.2.99
213.204.2.100
213.204.2.101

Tabella 3: Gli IP target dell'analisi di sicurezza

Tutte le attività sono state realizzate da una postazione di attacco (di proprietà di Hacking Team) appositamente configurata. Tale postazione è costituita da due piattaforme: Linux Fedora 7 e Windows XP Professional, entrambi equipaggiati con gli strumenti necessari per la realizzazione delle verifiche di sicurezza.

Nel seguente diagramma viene schematizzato l'ambiente in cui sono state eseguite le attività di *test*, ed i *target* di verifica più significativi a livello di topologia:

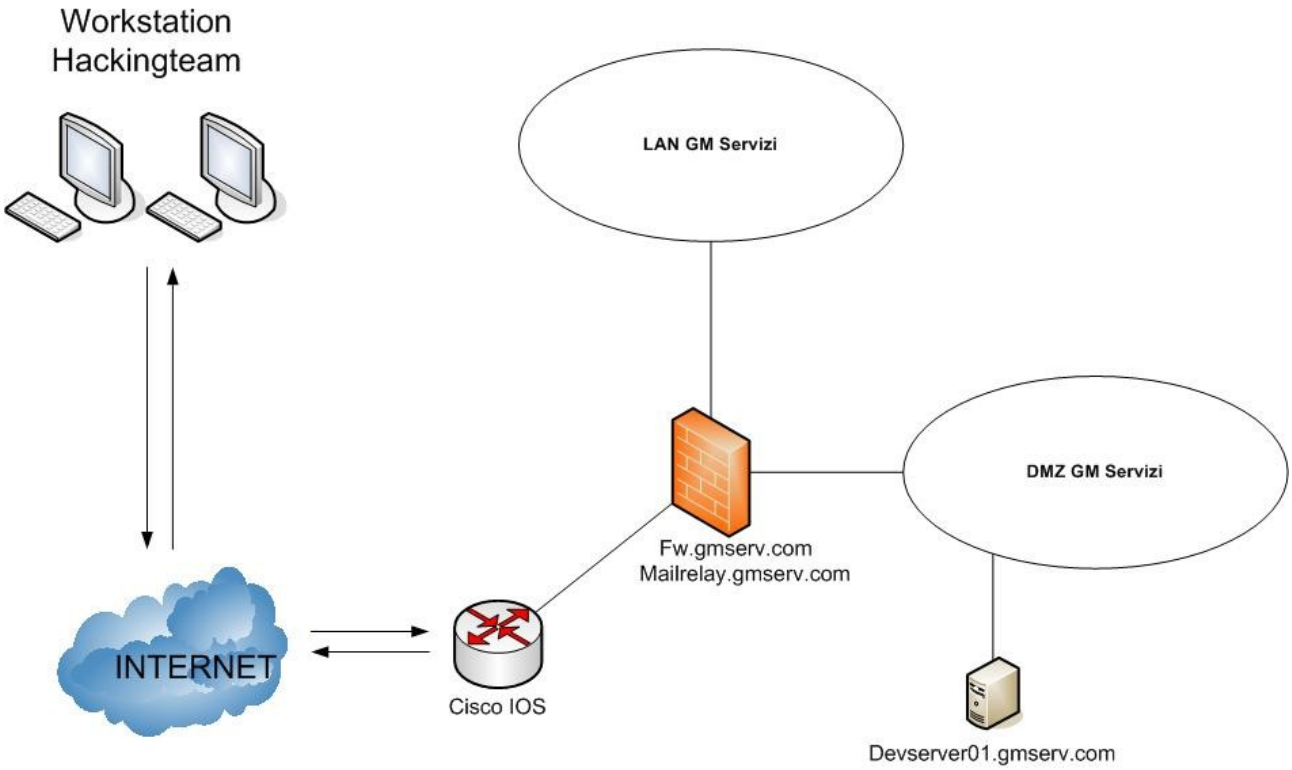

Figura 3 - Schema di rete

2 Test effettuati

2.1 Attività eseguite

Le attività di verifica sono state condotte utilizzando tecniche di attacco allo stato dell'arte, e seguendo un approccio metodologico di tipo manuale e/o automatico, a seconda delle singole attività. Tipicamente gli approcci possibili sono i seguenti:

- Modalità manuale
- Modalità automatica (utilizzo di vari tool di verifica)
- Modalità automatica combinata con interventi manuali. In questo caso alcuni strumenti automatici assistono il *tester*, nell'implementazione di uno scenario di attacco complesso.

La sequenza di macro-attività effettuate è descritta nella seguente figura:

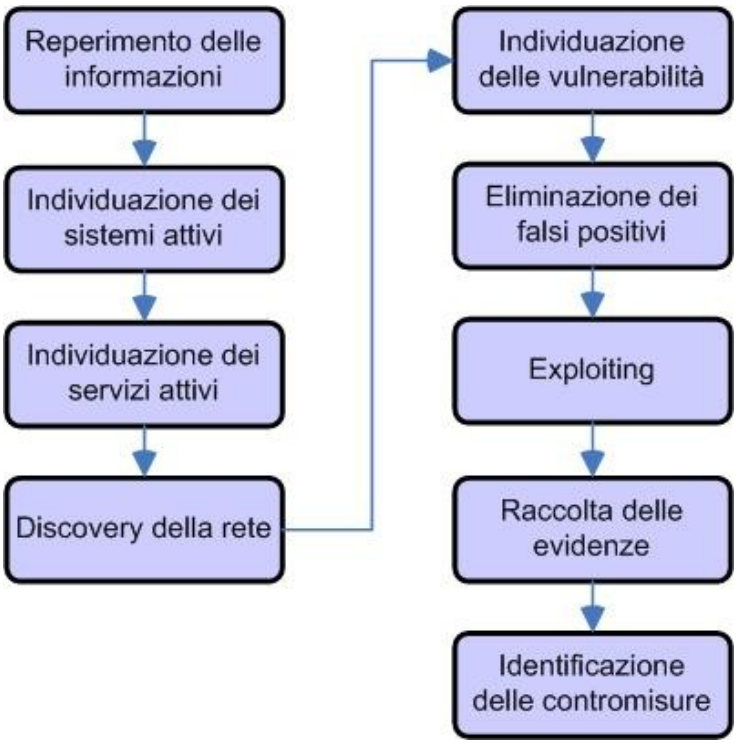

Figura 4: attività effettuate

2.2 Tools utilizzati

Gli strumenti di *vulnerability assessment* utilizzati sono i seguenti:

- ***System vulnerability scanner:*** *tools* di scansione automatica di sistemi operativi e reti che hanno come obiettivo la rilevazione di vulnerabilità note. I *tool* in questione generalmente utilizzano dei *plugin* appositamente codificati. E' stato utilizzato per lo più Nessus.
- ***Network discovery tools:*** strumenti e comandi che permettono di stabilire una probabile configurazione di rete a livello topologico ed architetturale. Sono stati utilizzati whois, traceroute, hping.
- ***Network mapping tools:*** *tools* che eseguono una scansione di singoli sistemi oppure intere reti al fine di determinarne le porte aperte, le applicazioni che sono in ascolto su quelle porte, il tipo e la versione

probabile del sistema operativo, ecc. Durante questo progetto i *tools* utilizzati sono stati nmap e tcptraceroute.

- ***Web application scan:*** strumento che permette l'analisi di applicazioni web e web services in modo semi-automatico. E' stato utilizzato principalmente Appscan.

3 Vulnerabilità riscontrate

3.1 DNS Zone Transfer

3.1.1 Descrizione

E' stato possibile enumerare l'elenco completo dei nomi a dominio per *gmserv.com* permettendo di conoscere i relativi indirizzi IP pubblicati nell'infrastruttura del Cliente. Questa debolezza implementativa fornisce una base di partenza notevole nel mapping della rete target sia dal punto di vista della semplice lista di indirizzi IP tenuti in considerazione durante le eventuali successive fasi dell'analisi, sia dal punto di vista qualitativo, ovvero rivelando nomi di solito pertinenti alla funzione stessa del server (ad es. *mailrelay.gmserv.com*).

La vulnerabilità è stata riscontrata sul server 213.204.2.59 porta 53/tcp**.**

Livello	Descrizione	Minaccia	Contromisura
Basso	Consente ad un attaccante il reperimento di informazioni sulla topologia dell'infrastruttura di rete del Cliente	Esporre informazioni specifiche sulla presenza di macchine attive sulla rete del cliente e permetterne il successivo attacco	Modificare la configurazione del DNS per permettere le zone transer solo ai DNS che effettivamente hanno necessità di tale operazione (ad es. i secondari)

3.1.2 Evidenze

```
> ls -d gmserv.com
[devserver01.gmserv.com]
 gmserv.com.                SOA    dns.gmserv.com gm.gmserv.com. (548 3600 6
00 86400 3600)
 gmserv.com.                NS     dns.gmserv.com
 gmserv.com.                NS     ns02.eurohosting.it
 gmserv.com.                NS     ns03.eurohosting.it
 gmserv.com.                MX     20   mailrelay.gmserv.com
 gmserv.com.                MX     30   mail.gmserv.com
 2000server                 A      213.204.2.61
 admin-carli-com            A      213.204.2.62
 admin-uno-it               A      213.204.2.59
 amgaservice-internetglobalservice-it A      213.204.2.59
 arca-internetglobalservice-it  A      213.204.2.62
 assonautica-im_it          A      213.204.2.59
 cadp-actelion-com          A      213.204.2.59
 cadp-actelion-jp-com       A      213.204.2.59
 cadp2-actelion-com         A      213.204.2.59
 ceg-internetglobalservice-it   A      213.204.2.62
 chorus-e-crf-it            A      213.204.2.59
 chorusdpp-e-crf-it         A      213.204.2.59
 circoloparasio_it          A      213.204.2.61
 clienti-carli-im           A      213.204.2.61
 cmr-clima_it               A      213.204.2.61
 dnndemo                    A      213.204.2.62
 dns                        A      213.204.2.60
 dns2                       A      213.204.1.193
 docks-ecodatamanager-it        A      213.204.2.59
 dpp                        A      213.204.2.60
 dpp-inkdata-eu             A      213.204.2.62
 dpp2-inkdata-eu            A      213.204.2.59
 dppbox                     A      213.204.2.62
 dppservices-actelion-com       A      213.204.2.59
 edilcm-internetglobalservice-it A      213.204.2.59
 edm-ecodatamanager-it          A      213.204.2.59
 essea-ecodatamanager-it        A      213.204.2.59
 fastweb-internetglobalservice-it A      213.204.2.59
 gaslini-internetglobalservice-it A      213.204.2.62
 giuliani-e-crf-it          A      213.204.2.59
 giulianiqa-e-crf-it        A      213.204.2.59
 gm-sms-service             A      213.204.2.62
 hotelcrocedimalta_com          A      213.204.2.59
 ibd-e-crf-it               A      213.204.2.59
 icems-ecodatamanager-it        A      213.204.2.59
 idroedil-ecodatamanager-it     A      213.204.2.59
 igs-internetglobalservice-it   A      213.204.2.62
 intra-fllicarli-im         A      213.204.2.62
 intra1-fllicarli-im        A      213.204.2.62
 itol-sms-service           A      213.204.2.62
 laportadeisapori_com           A      213.204.2.59
 levelip-sms-service        A      80.247.73.55
 levelip-sms-service2       A      80.247.73.82
 mail                       A      213.204.1.2
 mailrelay                  A      213.204.2.58
 maugeri-e-crf-it           A      213.204.2.59
 maugeriqa-e-crf-it         A      213.204.2.59
 multiservizi-internetglobalservice-it A      213.204.2.62
```

ninosanremo A 213.204.1.70
nyala-highlight A 213.204.2.61
ordini-carli-im A 213.204.2.59
phone-uno-it A 213.204.2.59
provfi-internetglobalservice-it A 213.204.2.62
provfi1-internetglobalservice-it A 213.204.2.62
provge-internetglobalservice-it A 213.204.2.59
provlu-internetglobalservice-it A 213.204.2.62
provpd-internetglobalservice-it A 213.204.2.59
registry-e-crf-it A 213.204.2.62
rivieraholidays_it A 213.204.2.59
router A 213.204.2.59
rse-ecodatamanager-it A 213.204.2.59
safety-e-crf-it A 213.204.2.59
serviziglobali_org A 213.204.2.61
sige A 80.247.73.58
sige2005 A 213.204.2.62
sigesvi A 213.204.2.62
sm-internetglobalservice-it A 213.204.2.59
stat A 213.204.1.26
test2000 A 213.204.2.61
testdevserver02 A 213.204.2.62
traspo-fllicarli-im A 213.204.2.62
trials-actelion-com A 213.204.2.59
uno-sms-service A 213.204.1.205
www A 213.204.1.193
www-actelion-jp-com A 213.204.2.61
www-arquistudioconsulting-com A 213.204.2.59
www-campingmistral-it A 213.204.2.59
www-carli-com A 213.204.2.62
www-cciaa-imperia-com A 213.204.2.59
www-cofarm-srl-it A 213.204.2.59
www-comune-alassio-sv-it A 213.204.2.59
www-consorziosantamaria-it A 213.204.2.62
www-coralloimperia-it A 213.204.2.59
www-didiesse-com A 213.204.2.59
www-dimeco-it A 213.204.2.59
www-e-crf-it A 213.204.2.59
www-ecodatamanager-it A 213.204.2.59
www-empolio-com A 213.204.2.59
www-essenzebioarredo-it A 213.204.2.62
www-freedogs-org A 213.204.2.62
www-globalservice-org A 213.204.2.62
www-globalservice-tv A 213.204.2.59
www-gmserv-com A 213.204.2.59
www-hippocrates-research-it A 213.204.2.59
www-hotel-rossini-it A 213.204.2.59
www-hotelcrocedimalta-com A 213.204.2.59
www-hotelduparc-it A 213.204.2.59
www-hotelstellamaris-info A 213.204.2.59
www-idroedil-info A 213.204.2.59
www-ilfaggiocoldinava-it A 213.204.2.59
www-ilfaggiocoop-it A 213.204.2.59
www-im-camcom-it A 213.204.2.59
www-immobiliareconte-com A 213.204.2.59
www-inkdata-eu A 213.204.2.62
www-internetglobalservice-it A 213.204.2.59
www-italgrafspa-com A 213.204.2.59
www-itol-tv A 213.204.2.62

```
www-leautomobili-it          A      213.204.2.59
www-lineamediterranea-it     A      213.204.2.62
www-lineamediterranea-net    A      213.204.2.62
www-maremoto-it              A      213.204.2.59
www-museodellolivo-com       A      213.204.2.62
www-ninosanremo-com          A      213.204.2.101
www-northsailscosmetics-com  A      213.204.2.62
www-nyalahotel-it            A      213.204.2.59
www-oldanistyle-it           A      213.204.2.59
www-oliocarli-at             A      213.204.2.62
www-oliocarli-co-uk          A      213.204.2.62
www-oliocarli-com            A      213.204.2.62
www-oliocarli-de             A      213.204.2.62
www-oliocarli-fr             A      213.204.2.62
www-oliocarli-it             A      213.204.2.62
www-olioliva-tv              A      213.204.2.62
www-oliveoil-org             A      213.204.2.59
www-papone-it                A      213.204.2.62
www-portodimperia-it         A      213.204.2.59
www-rivieragas-it            A      213.204.2.59
www-rosa-mystica-it          A      213.204.2.62
www-royalhotelsanremo-com    A      213.204.2.59
www-san-damian-com           A      213.204.2.59
www-seliteskudotech-it       A      213.204.2.62
www-starmilanofiori-it       A      213.204.2.59
www-studiobruna-it           A      213.204.2.59
www-studiocorio-it           A      213.204.2.59
www-tinstabile-it            A      213.204.2.59
www-uno-it                   A      213.204.2.59
www-veledepoca-com           A      213.204.2.59
www1-carli-com               A      213.204.2.62
www2-carli-com               A      213.204.2.62
zambongroup-e-crf-it         A      213.204.2.59
gmserv.com.                  SOA    dns.gmserv.com gm.gmserv.com. (548 3600 6
00 86400 3600)
>
```

Figura 5 – Elenco degli host del dominio gmserv.com

3.2 Open DNS

3.2.1 Descrizione

Il server DNS risponde anche per domini per i quali non è autoritativo permettendo così di effettuare attacchi verso terzi a partire da un indirizzo IP registrato a nome di GM Servizi e cioé proprio quello del DNS.
Inoltre questo potrebbe permettere l'effettuazione di attacchi di tipo DNS spoofing verso gli utilizzatori di tale DNS (principalmente i client della rete di GM Servizi) reindirizzandoli verso siti diversi da quelli corretti.

La vulnerabilità è stata riscontrata sul server 213.204.2.59 porta 53/tcp**.**

Livello	Descrizione	Minaccia	Contromisura
Medio	Consente di effettuare attacchi di tipo Denial of Service verso terze parti o verso il cliente stesso	Esporre GM Servizi ad essere utilizzata come ponte per attacchi *DoS*	Modificare la configurazione del DNS server per limitare la risoluzione dei nomi Internet al più alle reti interne del Cliente.

3.2.2 Evidenze

nslookup www.repubblica.it 213.204.2.59

Server: devserver01.gmserv.com
Address: 213.204.2.59

Risposta da un server non di fiducia:
Nome: repubblica.it
Address: 75.126.144.219
Aliases: www.repubblica.it

3.3 SQL Injection

3.3.1 Descrizione

La scheda prodotto del sito "*ninosanremo*", sembra essere vulnerabile ad un attacco SQL injection sul campo *ID*, che potrebbe permettere l'accesso al DB senza l'utilizzo di credenziali.
La complessità della query vulnerabile (in rapporto quindi all'insieme di campi che formano la scheda prodotto risultante da una serie di join di differenti tabelle) in relazione al tempo a disposizione, non ha permesso di ottenere un risultato di completa compromissione del Database. E' plausibile affermare però che con un effort ed un tempo maggiore a disposizione la compromissione del DB sarebbe stata probabile.

La URL vulnerabile è (ad esempio): http://213.204.2.101/www-ninosanremo-com/scheda.php?id=300

La vulnerabilità è stata riscontrata sul server 213.204.2.101 porta 80/tcp**.**

Livello	Descrizione	Minaccia	Contromisura
Medio	E' possibile eseguire *query* SQL sul database dell'applicazione dal Web	E' possibile interagire con il Database e comprometterne la relativa sicurezza avendo accesso a tutti i dati in esso contenuti	Modificare la validazione dell'input del campo ID per accettare solo valori numerici o che comunque non permettano di accodare istruzioni poi passate al DB

3.3.2 Evidenze

Figura 6 - SQL Injection e codice di errore restituito

3.4 Source Code Disclosure

3.4.1 Descrizione

E' possibile visualizzare il codice sorgente di alcune applicazioni web. Questo espone la logica applicativa ad un'analisi da parte di un attaccante e potrebbe rivelare eventuali credenziali cablate nel programma.

I file trovati con queste caratteristiche sono:

http://213.204.2.101 /www-ninosanremo-com/index_menu.php.old
http://213.204.2.101 /www-ninosanremo-com/mondo_rosa.php.old

http://213.204.2.101 /www-ninosanremo-com/coltivazione.php.old
http://213.204.2.101 /www-ninosanremo-com/form_ordine.php.old

Le versioni (vista l'estensione dei file stessi) non è certamente l'ultima in linea, ma potrebbe contenere informazioni preziose per lo scopo descritto sopra.

La vulnerabilità è stata riscontrata sul server 213.204.2.101 porta 80/tcp**.**

Livello	Descrizione	Minaccia	Contromisura
Medio	E' possibile visualizzare il codice sorgente di alcune applicazioni web	E' possibile effettuare reverse engineering sulla logica dell'applicazione nonché scoprire credenziali hard coded	Impostare correttamente i permessi di accesso ai file e rimuovere i file contenenti i sorgenti delle applicazioni non più utilizzati

3.4.2 Evidenze

Di seguito viene riportato un stralcio del file *form_ordine.php.old*

```
<?php
require_once("./config.php");
include(MAIN_SQL_CONN);
include("./basket.php");

session_name("nino");
session_start();

$gran_totale = $_SESSION['basket']->Get_Tot_Price();
if ($_SESSION['basket']->Get_Order_Id() != 0) {
        $id_ordine = $_SESSION['basket']->Get_Order_Id();

        $query_dati_ordine = "SELECT * FROM ordini WHERE id_ordine=".$id_ordine;
        $result_dati_ordine = mysql_query($query_dati_ordine) or die(mysql_error());
        $array_dati_ordine = mysql_fetch_array($result_dati_ordine);
}
/*
 else {
        $id_ordine = 0;
}
*/
?>
<html>
<head>
```

```
<title>Nino Sanremo</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="stili.css" rel="stylesheet" type="text/css">

<script language="javascript">
// <!--
function checkChar(str) {
/*********************************************
La seguente funzione riceve come parametro una stringa
ed esclude, entrando nella condizione if, i caratteri
definiti dall'espressione regolare; poi, sempre all'interno
dell'if, imposta una variabile a false che restituirà
alla fine della funzione.
*********************************************/
        controllo = true;
        l_str = str.length;
        for (i=0; i < l_str; i++) {
                a = str.charAt(i);
                var RegExp=/[^a-z^A-Z^\-^\_^\.^0-9]/;
        if (RegExp.test(a)) {
                        alert("Il carattere " + a + " non è permesso nei nomi di files.");
                        controllo = false;
                }
 }
 return controllo;
}
```

3.5 Metodi TRACE e TRACK HTTP abilitati

3.5.1 Descrizione

I metodi TRACE e TRACK sono utilizzati principalmente per il debugging delle applicazioni.

In particolare, forniscono al client una sorta di loopback delle sue richieste così come vengono ricevute dal server. TRACE è un metodo standard definito da una RFC (2616) mentre TRACK è il metodo equivalente implementato da Microsoft.

Tramite il loopback delle richieste è possibile eseguire del codice nel browser dei client ed impadronirsi di informazioni sensibili quali host-header, cookies, etc..

La vulnerabilità è stata riscontrata sul server devserver01.gmserv.com porta 80/TCP.

Livello	Descrizione	Minaccia	Contromisura
Basso	I metodi TRACE e TRACK sono abilitati per il debugging delle applicazioni Web	Si possono teoricamente ottenere informazioni sensibili lato client	Modificare il file di configurazione del Web server disabilitando i metodi TRACE e TRACK

Nonostante questa debolezza sia difficilmente sfruttabile (per questo motivi il relativo livello di rischio è stato classificato come *"basso"*), si consiglia comunque di disabilitare i metodi sopracitati.

3.5.2 Evidenze

Di seguito viene riportato l'output di una risposta da parte del server Web ad una richiesta TRACE del client (tool di scansione automatico in questo caso):

TRACE /Nessus481.html HTTP/1.1
connection: Keep-Alive
host: devserver01.gmserv.com
pragma: no-cache
user-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
accept-language: en
accept-charset: iso-8859-1,*,utf-8

4 Stato dei sistemi

I sistemi risultati vulnerabili sono riassunti nella seguente tabella.

Rete	Indirizzo IP	Vulnerabilità
GM Servizi	213.204.2.59	V1
GM Servizi	213.204.2.59	V2
GM Servizi	213.204.2.101	V3
GM Servizi	213.204.2.101	V4
GM Servizi	213.204.2.60	V5

Tabella 4: Vulnerabilità riscontrate

4.1 GM Servizi

La fase iniziale di mappatura della rete oggetto dell'analisi è stata svolta mediante interrogazioni al Domain Name System ed al database pubblico WHOIS. Il risultato della richiesta è il seguente:

4.1.1 Discovery della rete

Per la prima network:

Information related to '213.204.2.48 - 213.204.2.63'

inetnum: *213.204.2.48 - 213.204.2.63*
netname: *GMSERVIZI-IM*
descr: *GM SERVIZI S.R.L.*
descr: *Via IV Novembre 71*
descr: *18100 Imperia*
descr: *Internal Network*
country: *IT*
admin-c: *CC845-RIPE*
tech-c: *BB84-RIPE*
status: *ASSIGNED PA "status:" definitions*
mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

person: *Carlo Capacci*
address: *Uno Communications S.p.A.*
address: *Licensed Telecommunications Operator*
address: *Wireless Local Loop Regional Company*
address: *Via Don Bellone 14*
address: *18100 IMPERIA*
address: *Italy*
address: *http://www.uno.it*
phone: *+39 0183 57000*
fax-no: *+39 0183 766182*
e-mail: *carlo.capacci@uno.it*
nic-hdl: *CC845-RIPE*
mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

person: *Berardo Bonaduce*
address: *Uno Communications S.p.A.*
address: *Licensed Telecommunications Operator*
address: *Wireless Local Loop Regional Company*
address: *Via Don Bellone 14*
address: *18100 IMPERIA*
address: *Italy*
address: *http://www.uno.it*
phone: *+39 0183 57000*
fax-no: *+39 0183 766182*
e-mail: *berardo.bonaduce@uno.it*
nic-hdl: *BB84-RIPE*
mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

% Information related to '213.204.0.0/19AS9137'

route: *213.204.0.0/19*
descr: *UNO COMMUNICATIONS NETWORK*
descr: *Uno Communications S.p.A.*
descr: *Licensed Telecommunications Operator*
origin: *AS9137*
remarks: *Send report of network abuse/spam*
remarks: *only to: abuse@uno.it*
remarks: *If you report abuse to any other address*
remarks: *you will get no response.*
mnt-by: *UNO-MNT*

source: *RIPE* *#* *Filtered*

Per la seconda network:

Information related to '213.204.2.96 - 213.204.2.111'

inetnum: *213.204.2.96 - 213.204.2.111*
netname: *GM-SERV-NET2*
descr: *Sottorete 2 cliente GMservizi*
country: *IT*
admin-c: *CC845-RIPE*
tech-c: *GG2885-RIPE*
status: *ASSIGNED PA "status:" definitions*
mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

person: *Carlo Capacci*
address: *Uno Communications S.p.A.*
address: *Licensed Telecommunications Operator*
address: *Wireless Local Loop Regional Company*
address: *Via Don Bellone 14*
address: *18100 IMPERIA*
address: *Italy*
address: *http://www.uno.it*
phone: *+39 0183 57000*
fax-no: *+39 0183 766182*
e-mail: *carlo.capacci@uno.it*
nic-hdl: *CC845-RIPE*
mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

person: *Gabriele Guasco*
address: *Uno Communications S.p.A.*
address: *Licensed Telecommunications Operator*
address: *Wireless Local Loop Regional Company*
address: *Via Don Bellone 14*
address: *18100 IMPERIA*
address: *Italy*
address: *http://www.uno.it*
phone: *+39 0183 57000*
fax-no: *+39 0183 767203*
e-mail: *gabriele.guasco@uno.it*
nic-hdl: *GG2885-RIPE*

mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

% Information related to '213.204.0.0/19AS9137'

route: *213.204.0.0/19*
descr: *UNO COMMUNICATIONS NETWORK*
descr: *Uno Communications S.p.A.*
descr: *Licensed Telecommunications Operator*
origin: *AS9137*
remarks: *Send report of network abuse/spam*
remarks: *only to: abuse@uno.it*
remarks: *If you report abuse to any other address*
remarks: *you will get no response.*
mnt-by: *UNO-MNT*
source: *RIPE # Filtered*

Per una corretta ricostruzione del disegno architetturale della rete remota, la tecnica utilizzata è la modulazione del TTL (time to live) dei pacchetti. La generazione di pacchetti aventi TTL differenti, è stata indirizzata verso i servizi pubblicamente raggiungibili della rete.
Di seguito vengono riportati graficamente i risultati ottenuti

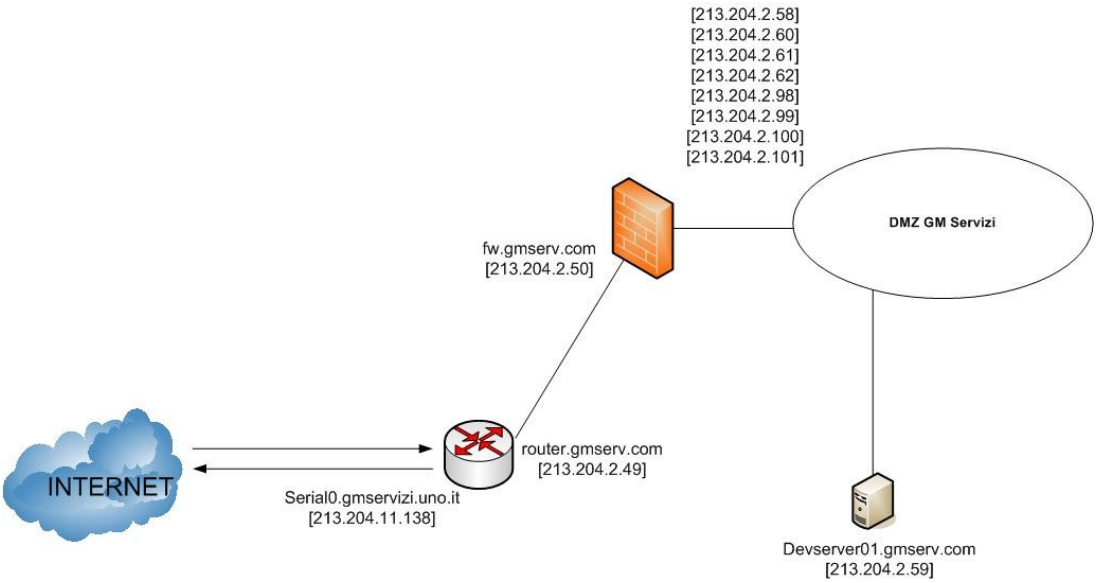

Figura 7 - Output grafico

4.1.2 Server 213.204.2.49

Info Generali		
OS fingerprint	Cisco router IOS 12.x	
Open **TCP** services	**Port Number**	**Service**
	23	Telnet
	Port Number	**Service**
Open **UDP** services Open **TCP** services		

E' stato trovato aperto il solo servizio telnet. L'apparato non accetta login anonimi e non sono state trovate conbinazioni di username/password banali.
Non è stata riscontrata alcuna vulnerabilità per questo servizio.

4.1.3 Firewall 213.204.2.50

Info Generali		
OS fingerprint	?	
	Port Number	Service
Open services	N/A	
Open **TCP** services		

Il sistema avente indirizzo IP 213.204.2.50, non espone alcun servizio. Da questa informazione e dalla risoluzione DNS inversa per questo host (*fw.gmserv.com*) si può verosimilmente ipotizzare che sia un apparato firewall.

4.1.4 Mail Relay 213.204.2.58

Info Generali		
OS fingerprint	Fortinet firewall ?	
Open **TCP** services	Port Number	Service
	25	smtp

Questo sistema espone il servizio SMTP (mail) e risulta essere risolto come *mailrelay.gmserv.com*
Il sistema operativo riconosciuto dai tools di scanning utilizzati ipotizza si tratti di un apparato Fortigate; se questa informazione risulta corretta il device stesso rappresenta il mail relay per la rete di GM Servizi (piuttosto che fornire NAT per un server mail relay a se stante).
Non sono state riscontrate debolezze né misconfigurazioni per questo servizio.
Il banner esposto è il seguente:

220 mailrelay.gmserv.com ESMTP SKMX/2.0

4.1.5 Devserver01 213.204.2.59

Info Generali		
OS fingerprint	Microsoft Windows	
Open **TCP** services	Port Number	Service
	80	http
	53	DNS
Open **UDP** services	53	DNS

L'indirizzo 213.204.2.59 risponde al nome *devserver01* ed espone un servizio web ed un servizio di risoluzione dei nomi (DNS).

Servizio web:
questo servizio presenta una pagina di errore dalla quale si deduce la presenza di un filtraggio a livello IP ADDRESS ACL (da parte del Web Server); non essendo evidentemente inclusi nella lista di indirizzi autorizzati, viene restituito il seguente messaggio:

You are not authorized to view this page

You do not have permission to view this directory or page from the Internet address of your Web browser.

If you believe you should be able to view this directory or page, please contact the Web site administrator by using the e-mail address or phone number listed on the 213.204.2.59 home page.

HTTP 403.6 - Forbidden: IP address rejected
Internet Information Services

Technical Information (for support personnel)

- Background:
  This error is caused when the server has a list of IP addresses that are not allowed to access the site, and the IP address you are using is in this list.
- More information:
  Microsoft Support

Non sono state riscontrate vulnerabilità per questo servizio.

servizio DNS

Sono state riscontrate le seguenti problematiche:

- Open DNS (si faccia riferimento al paragrafo 3.2 per maggiori dettagli)
- DNS Zone Transfer (si faccia riferimento al paragrafo 3.1 per maggiori dettagli)

4.1.6 213.204.2.60

Info Generali		
OS fingerprint	?	
Open **TCP** services	Port Number	Service
	80	http

Questo host espone un servizio web http. Sono state riscontrate le seguenti debolezze:

- I metodi HTTP TRACE e TRACK sono abilitati

4.1.7 213.204.2.61

Info Generali		
OS fingerprint	?	
Open **TCP** services	Port Number	Service
	80	http

Nonostante il servizio sia aperto, è "tcpwrapped", ovvero il server non accetta di fatto connessioni dagli indirizzi ip utilizzati per effettuare i test

4.1.8 213.204.2.62

Info Generali		
OS fingerprint	**Microsoft Windows**	
Open **TCP** services	Port Number	Service
	80	http

L'indirizzo 213.204.2.62 risponde al nome "*admin-carli-com.gmserv.com*" ed espone un servizio web basato su Microsoft Internet Information Server.

Questo servizio presenta una pagina di errore dalla quale si deduce la presenza di un filtraggio (applicativo) a livello IP ADDRESS ACL; non essendo evidentemente inclusi nella lista di indirizzi autorizzati, viene restituito il seguente messaggio:

You are not authorized to view this page

The Web server you are attempting to reach has a list of IP addresses that are not allowed to access the Web site, and the IP address of your browsing computer is on this list.

Please try the following:

- Contact the Web site administrator if you believe you should be able to view this directory or page.

HTTP Error 403.6 - Forbidden: IP address of the client has been rejected.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **About Security**, **Limiting Access by IP Address**, **IP Address Access Restrictions**, and **About Custom Error Messages**.

4.1.9 213.204.2.98

Info Generali		
OS fingerprint		
Open **TCP** services	Port Number	Service

Questo indirizzo non espone alcun servizio

4.1.10 213.204.2.99

Info Generali		
OS fingerprint		
Open **TCP** services	Port Number	Service

Questo indirizzo non espone alcun servizio

4.1.11 213.204.2.100

Info Generali		
OS fingerprint		
Open **TCP** services	Port Number	Service

Questo indirizzo non espone alcun servizio

4.1.12 www-ninosanremo-com.gmserv.com 213.204.2.101

Info Generali		
OS fingerprint	**Microsoft Windows**	
Open **TCP** services	Port Number	Service
	80	http

L'indirizzo IP 213.204.2.101 risponde al nome di "*www-ninosanremo-com.gmserv.com*" ed espone un servizio web basato su piattaforma Apache/2.2.3 (Ubuntu) PHP/5.2.1

Sono state rilevate le seguenti vulnerabilità:

- SQL Injection (si faccia riferimento al paragrafo 3.3 per maggiori dettagli)
- Source code disclosure (si faccia riferimento al paragrafo 3.4 per maggiori dettagli)

5 Conclusioni e strategia di fixing

Nei due paragrafi che seguono vengono suddivise sia le strategie implementative per risolvere in modo puntuale le debolezze rilevate, sia quelle ad orientamento più generale,

Lo scopo di queste ultime è quello di porre rimedio da un punto di vista architetturale alle tematiche di sicurezza pertinenti all'infrastruttura del Cliente.

5.1 Fixing specifico per le problematiche riscontrate

N°	Categoria di vulnerabilità	Soluzione proposta
V1	DNS Zone Transfer	Modificare la configurazione del DNS per permettere le zone transer solo ai DNS che effettivamente hanno necessità di tale operazione (ad es. i secondari)
V2	Open DNS	Modificare la configurazione del DNS server per limitare la risoluzione dei nomi Internet al più alle reti interne del Cliente.
V3	SQL Injection	Per eliminare la vulnerabilità è necessaria la riscrittura del codice di interfacciamento fra le pagine WEB e il database SQL. Come ulteriore soluzione è possibile l'inserimento di un *application firewall* a monte del *web server*. Le due soluzioni non sono mutuamente esclusive.
V4	Source Code Disclosure	Impostare correttamente i permessi di accesso ai file e rimuovere i file contenenti i sorgenti delle applicazioni non più utilizzate.
V5	Metodi TRACE e TRACK HTTP abilitati	Disabilitare i metodi TRACE e TRACK modificando i files di configurazione del Web Server

Tabella 5: strategia di fixing

Dall'attività eseguita, il livello di sicurezza della rete di GM Servizi può essere completamente ripristinato con un minimo effort, come si evince dalla tabella sopra riportata "strategia di fixing".

5.2 *Security plan summary* per le problematiche riscontrate

La debolezza implementativa di alcune applicazioni, come ad esempio quelle web che accedono ai DataBase, può essere fortemente mitigata con l'utilizzo di strumenti e servizi; le principali tematiche che si consiglia di affrontare in tal senso sono le seguenti:

- Apparati di tipo "Application Firewall" (sia web, che DB)
- Ottimizzazione delle procedure di validazione delle applicazioni in pre-produzione
- Strumenti di analisi del codice o (a seconda della quantità di sviluppo interno) servizi consulenziali di *"code review"*
- Ottimizzazione delle procedure di *hardening e auditing* dei server