WORKSHOP GARR 2022

NET MAKERS

Simona Venuti

SCARR

- Perché
- Cosa
- Come
- Report
- Take Out

SCARR – SCAnsioni Ripetute a Richiesta

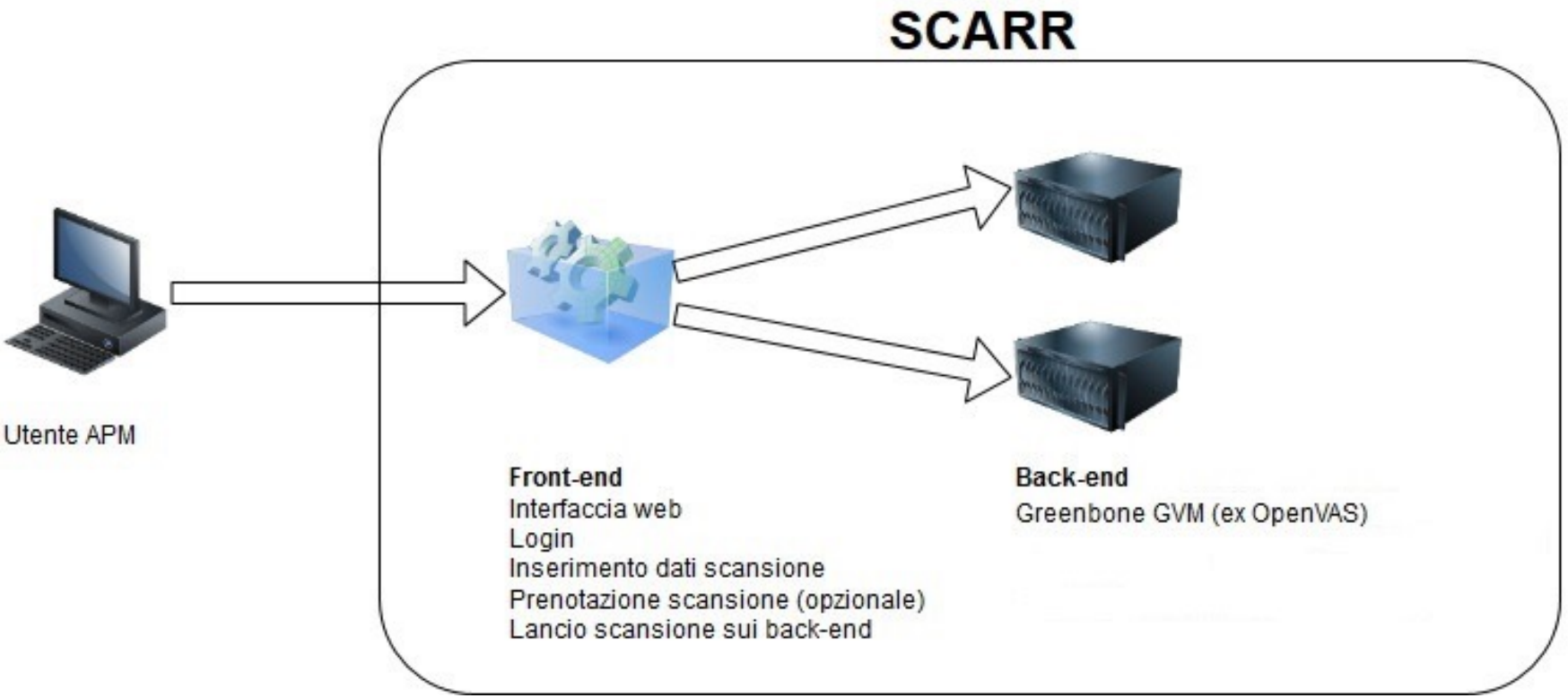
Scansioni vulnerabilità remote – Vulnerability Assessment

- Analisi del rischio
- Patch management
- Visibilità della propria rete dall'esterno
- Direttiva AGiD «Misure minime di sicurezza»

- Rivolto a tutti gli APM della rete GARR
- E' un servizio (SP) della Federazione IDEM, *richiede l'adesione ad IDEM con un IdP*
- Frontend creato da GARR DEVOPS, backend OpenVAS - GreenBone

https://scarr.garr.it

Architettura



Architettura – ON-DEMAND!

Un po’ di numeri – 2021

753 scansioni	**289 host singoli +** **464 reti di cui:** **2 /21** **19 /22** **83 /23** **268 /24** **43 /25** **24 /26** **6 /27** **15 /29** **4 /32**

- **Per un totale di 141.381 host**
  Da 560 sedi - 65 sedi diverse

Fase di autenticazione - login

- **Autenticazione:** L'utente fa login tramite IDEM

- **Autorizzazione:** vengono raccolti gli attributi dall'IdP:
  - **ePPN** (required) accesso al sistema
  - **mail** (required) per autorizzazione e ricevere notifiche
  - **surname** (required)
  - **givenName** (required)

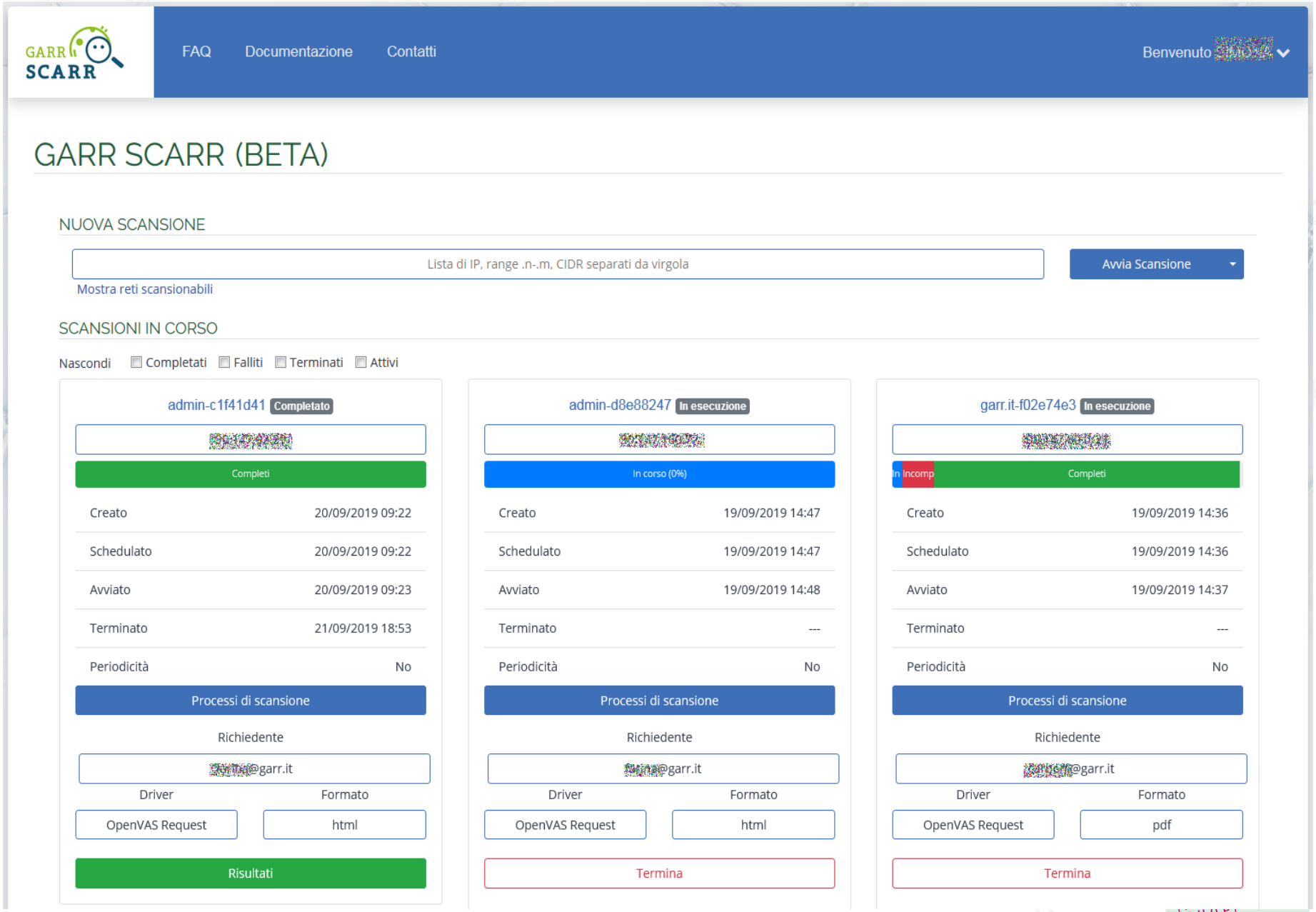
Fase di Autorizzazione - permessi

- Attraverso l'attributo mail, ricevuta dall'IdP, SCARR cerca di fare il match con le mail degli APM registrati in DB-GARR

Mail fornita dall'IdP: **venuti@garr.it**	↔	**Select mail, OrgNAME, Networks FROM APM.TABLE** **simona.venuti@garr.it ; GARR ; 10.2.0.0/24** **pippo.baudo@uniXX.it ; University of XX ; 10.x.x.x/16** **dino.zoff@uniYY.it ; University of YY ; 10.y.y.y/19**

- Se c'è match l'utente autenticato è anche autorizzato, e viene recuperata da GARRX-DB la sede dell'APM e le relative reti /CDIR di competenza

- Altrimenti il sistema restituisce un errore di **«non autorizzato»**
  - Non si è APM
  - L'indirizzo mail proveniente dall'IdP è diverso da quello in GARRX-DB


GARR SCARR
FAQ
Documentazione
Contatti
Benvenuto
GARR SCARR (BETA)
NUOVA SCANSIONE
Lista di IP, range .n-.m, CIDR separati da virgola
Avvia Scansione
Mostra reti scansionabili
SCANSIONI IN CORSO
Nascondi
Completati
Falliti
Terminati
Attivi
admin-c1f41d41
Completato
Completi
Creato 20/09/2019 09:22
Schedulato 20/09/2019 09:22
Avviato 20/09/2019 09:23
Terminato 21/09/2019 18:53
Periodicità No
Processi di scansione
Richiedente
@garr.it
Driver
Formato
OpenVAS Request
html
Risultati
admin-d8e88247
In esecuzione
In corso (0%)
Creato 19/09/2019 14:47
Schedulato 19/09/2019 14:47
Avviato 19/09/2019 14:48
Terminato ---
Periodicità No
Processi di scansione
Richiedente
@garr.it
Driver
Formato
OpenVAS Request
html
Termina
garr.it-f02e74e3
In esecuzione
In
Incomp
Completi
Creato 19/09/2019 14:36
Schedulato 19/09/2019 14:36
Avviato 19/09/2019 14:37
Terminato ---
Periodicità No
Processi di scansione
Richiedente
@garr.it
Driver
Formato
OpenVAS Request
pdf
Termina

Caratteristiche dei test

- Il servizio permette di scansionare solo IP, reti e sottoreti GARR della propria struttura
- Il servizio non permette di scansionare IP non GARR o non della propria struttura
- Vengono scansionate **tutte le porte TCP e Nmap top 100 UDP**
- Per ogni IP e per ogni porta più di **60.000 test di vulnerabilità**

Prenotazione e periodicità

Prenotazione scansioni: Effettuare la scansione non immediatamente ma ad una data/ora precisa

- *Per poter aprire il firewall di bordo*
- *Per non caricare troppo la rete durante l'orario di servizio*

Ripetizione automatica scansioni: Può essere utile effettuare le stesse scansioni a distanza regolare nel tempo

- Mensile, bimestrale, trimestrale, semestrale
- *Per tenere la situazione sotto controllo ad intervalli regolari*
- *Per ottemperare alle «misure minime di sicurezza»*

Risultati e report

Result Overview

Host	High	Medium	Low	Log	False Positive
[redacted]37	77	17	0	0	0
[redacted]98	4	2	0	0	0
Total: 2	81	19	0	0	0

- Vulnerabilità riscontrate per ogni nodo scansionato
- Ordinate secondo la severità
- Indicazioni dei rimedi disponibili per gestire ogni vulnerabilità

Report – Dettaglio vulnerabilità

High (CVSS: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:5.3.3
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 5.3.3
Fixed version: 5.6.7

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.7 or later.

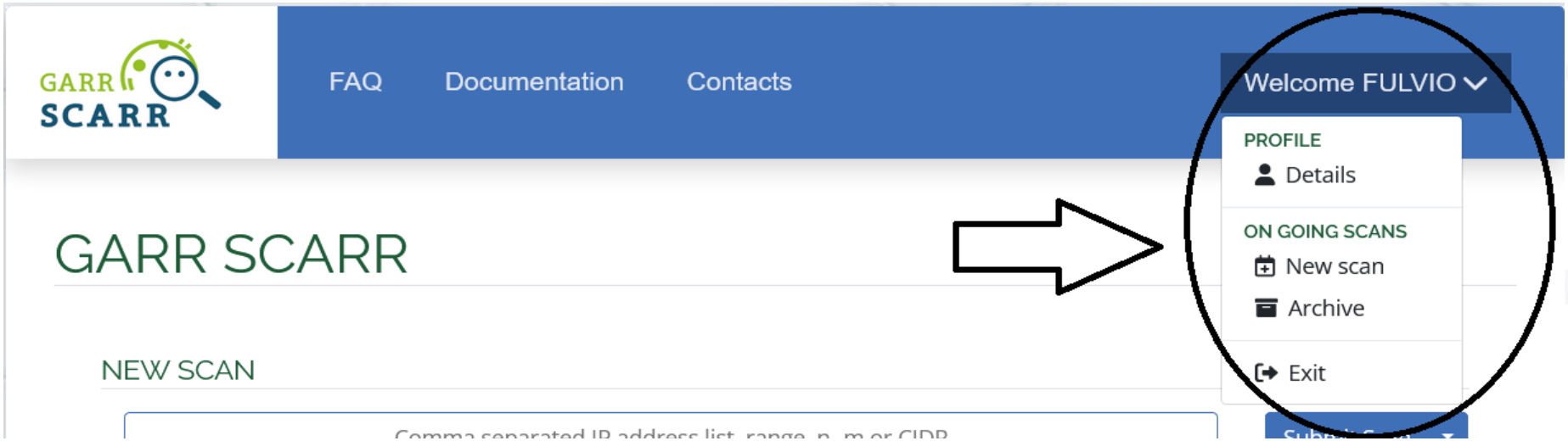
Affected Software/OS
PHP versions prior to 5.6.7 on Linux

Vulnerability Insight
The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP 'type confusion' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808673
Version used: $Revision: 14181 $

Product Detection Result
Product: cpe:/a:php:php:5.3.3
Method: PHP Version Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
CVE: CVE-2015-4601
BID:75246
Other:
URL:http://www.php.net/ChangeLog-5.php



- Selezionando **«PROFILO» - «Dettagli»** esce un piccolo pop-up

- La sede GARR di cui si è APM
- Il tipo di utenza SCARR (utente)
- Tutte le reti scansionabili dall'APM

Archivio scansioni

GARR SCARR

FAQ Documentazione Contatti Benvenuto SIMONA

GARR SCARR

Scarica archivio

TARGET	STATUS	TASKS	PERCENT	SCHEDULE_DATETIME	START_DATETIME	END_DATETIME	OWNER
[redacted]	Completato	4	100/0/0	29/08/2022 02:08	29/08/2022 02:08	29/08/2022 04:38	[redacted]
	Completato	8	100/0/0	29/08/2022 00:00	29/08/2022 00:00	29/08/2022 00:04	
	Completato	4	100/0/0	28/08/2022 02:07	28/08/2022 02:08	28/08/2022 04:52	
	Completato	8	100/0/0	28/08/2022 00:00	28/08/2022 00:00	28/08/2022 04:22	
	Completato	32	100/0/0	28/08/2022 00:15	28/08/2022 00:16	28/08/2022 02:26	

- Possono essere ordinate per qualsiasi campo
- **«SCARICA ARCHIVIO»** per scaricare tutto l'archivio in un foglio XLS (Excel)

Riferimenti

- GreenBoneGVM (ex OpenVAS): https://community.greenbone.net/t/about-gvm-architecture/1231
- GreenBone Source Edition (GSE) https://community.greenbone.net/c/gse/16

- Classificazione CVSS delle severità: https://www.first.org/cvss/v2/guide
- Mitre CVE: https://mitre.cve.org

- AUP GARR: https://www.garr.it/it/regole-di-utilizzo-della-rete-aup
- Trova il tuo APM: https://www.garr.it/it/comunita/la-comunita-garr/trova-il-tuo-apm
- Federazione IDEM GARR: https://www.idem.garr.it

https://learning.garr.it/media/VideoTutorialGenerici/SCARR/SCARR-Tutorial1/mail.html

SCARR - Scansioni Ripetute a Richiesta

Beta!

La tua rete è protetta?

Con SCARR, un nuovo servizio dedicato agli APM delle sedi GARR, puoi accorgerti di eventuali problemi di sicurezza all'interno della tua rete prima che lo facciano gli hacker.

Ho chiuso il ~~gas~~ ehm.. il firewall?

Con SCARR hai finalmente un modo semplice per avere una visione d'insieme di ciò che della tua rete esponi al mondo esterno: puoi facilmente pianificare test di sicurezza sulla tua rete. I test verranno eseguiti da postazioni site al di fuori della tua rete, al fine di simulare tentativi d'attacco reali: attacchi in cui gli eventuali malintenzionati mirerebbero ai punti deboli della tua rete per aprirsi backdoors.

Un sistemista fedele ...e sempre aggiornato!

"Avrò applicato su tutte le macchine gli aggiornamenti di sicurezza importanti per evitare l'exploit X di cui ho letto sulla mailing list Y?" "

Che sistema operativo e che applicazioni avranno mai installato quelli della farm Z? Come faccio a mantenere tutto ciò in sicurezza ? "

Servizio SCARR

> Accedi ora!

L'a tua username GarrSSO è S[EMAIL] l'accesso è riservato esclusivamente agli APM GARR

demandiamo al videotutorial sottostante per informazioni su come effettuare la richiesta d'accesso al servizio.

Tutorial SCARR

> Video tutorial

Contatti

Scrivere a:

scarr@garr.it

SCARR

- **https://scarr.garr.it**

- **https://scarr.garr.it/faq/**
- **https://scarr.garr.it/docs/**

scarr-service@garr.it