Cybersecurity nel Settore Sanitario Italiano: Esperienze sul Campo e Lezioni Apprese

Lorenzo Bracciale, Giuseppe Bianchi

CNIT Network Assessment, Assurance e Monitoring (NAM LAB)

1

Cyberthreats on Italian medical landscape

2019 – Popular Insulin Pump

- This wireless RF communication protocol does not properly authentication
- An attacker can control insulin delivery

The many Ransomware attacks

- Verona (2023), L'Aquila(2023), Basilicata (2024), Milano (2023) ...

What is the status of cyber-health of italian NHS?

2

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

1. Exposed PACS

3

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Where your X-Ray goes?

X-ray, MRI, CT

DICOM

PACS Server

(Picture Archiving and Communication System)

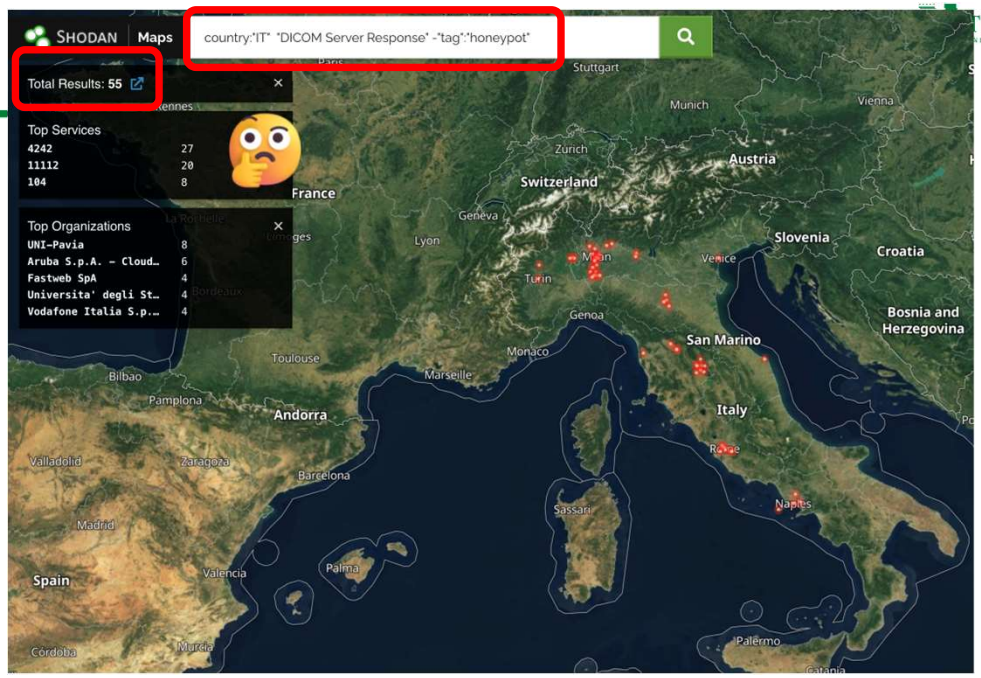
(DICOM Server)

DICOM

DICOM

PACS clients

4



5

What if some of them are left **open**?

6

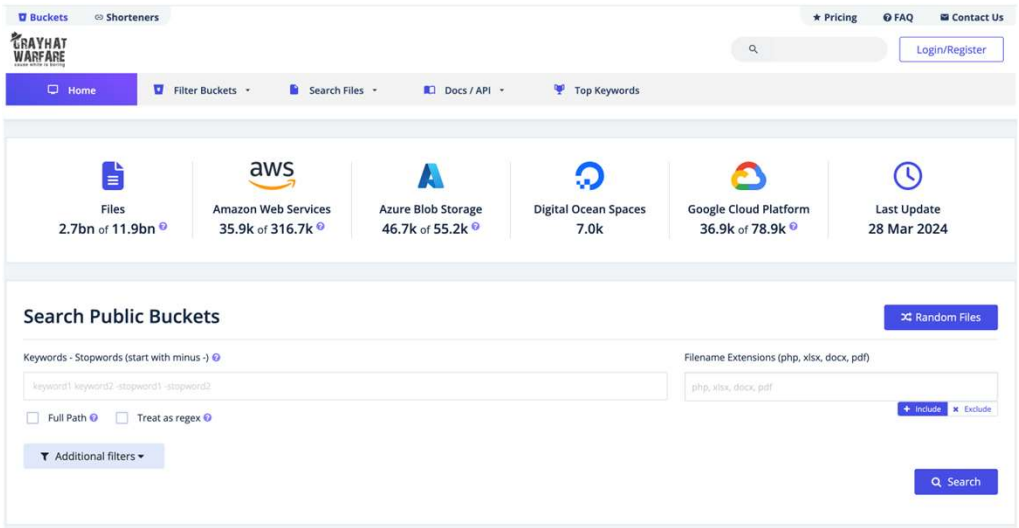
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

2. Medical Cloud Data

7

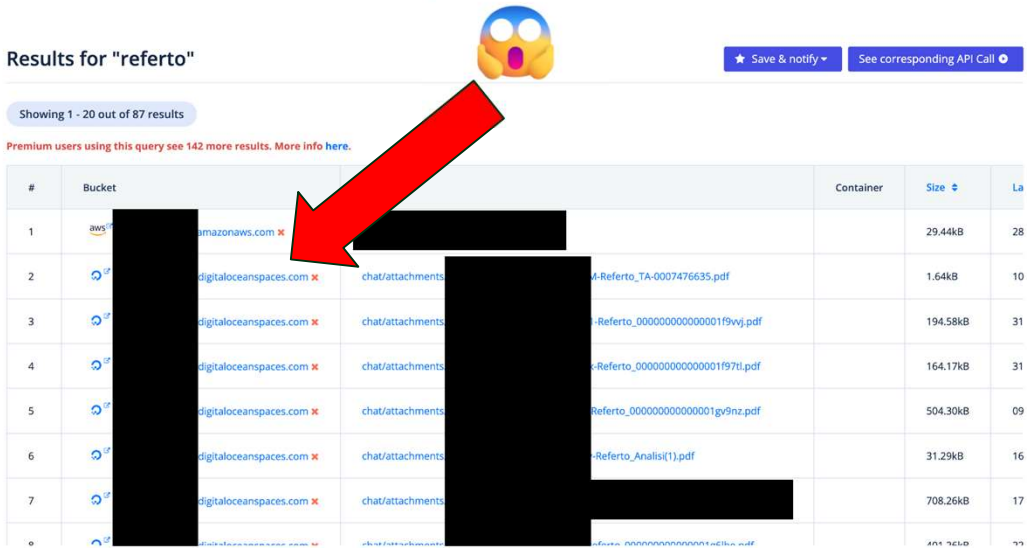
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Searching open buckets



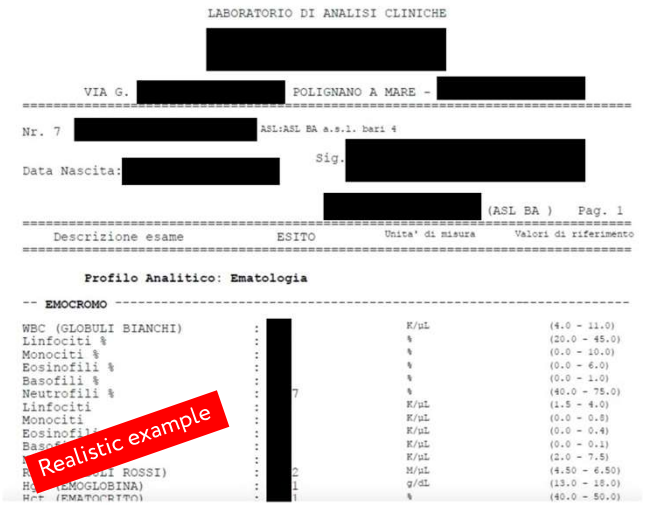
8

Searching for "medical report"



9

Exposed medical report: example



10

Searching for DICOM files

One million????!!!

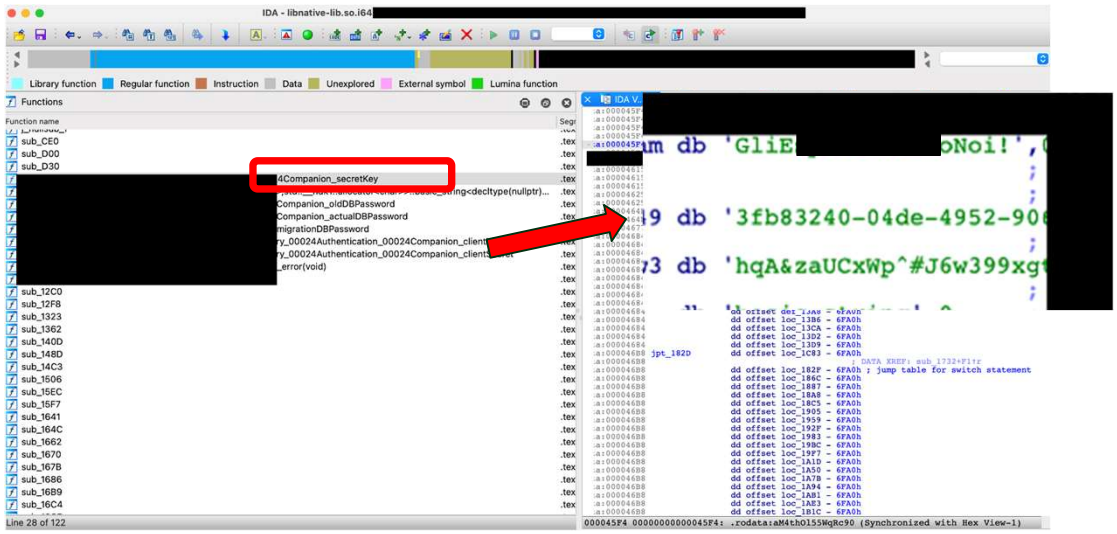
11

3. Medical Mobile Applications

12

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Hard-coded credentials



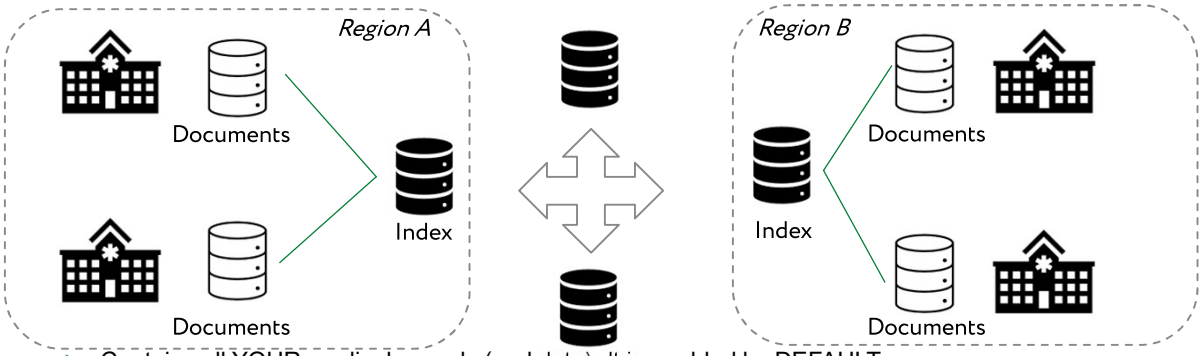
13

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

4. Electronic Health Records: A Tale of a Vulnerability

14

Italian Electronic Health Record (EHR/FSE)



- Contains all YOUR medical records (and data). It is enabled by DEFAULT.
- A wide access control policy: doctors, hospitals, ASL, pharmacies
- 20 different implementation for (almost) the same service (!)
- Technical changes + rush: a perfect explosive cocktail!
  - Next Generation EU (PNRR): target 85% of Patient Summary data by 2025 (Mission 6).
  - FSE 2.0 (new architecture).

15

User Data in EHR

Ministero della Salute

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

INTRODUZIONE

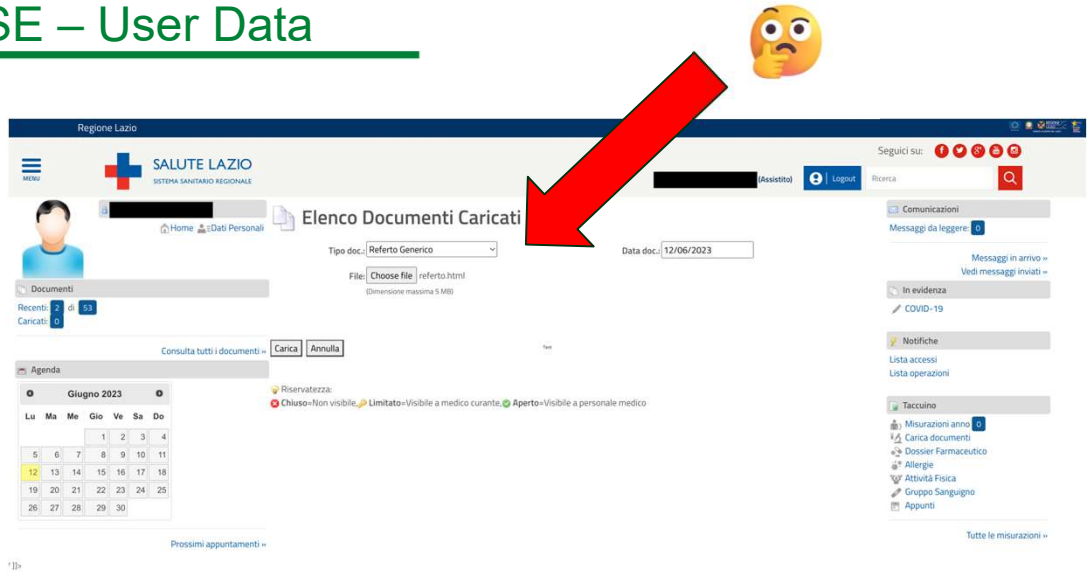
Definizione di Taccuino

Il DPCM 178/2015 definisce all'Art. 4 il "Taccuino personale dell'assistito" come sezione riservata del FSE all'interno della quale è permesso all'assistito di inserire dati e documenti personali relativi ai propri percorsi di cura, anche effettuati presso strutture al di fuori del SSN, precisando che i dati e i documenti inseriti nel taccuino sono informazioni non certificate e devono essere distinguibili da quelli inseriti dagli altri soggetti che concorrono all'alimentazione del FSE (definiti all'articolo 12 del medesimo Decreto).

Si tratta quindi di una sezione del FSE con caratteristiche profondamente differenti dalle altre, che debbono essere considerate nell'analisi dei contenuti informativi ed anche, in prospettiva, nella realizzazione dei servizi e nell'utilizzo delle informazioni ivi contenute.

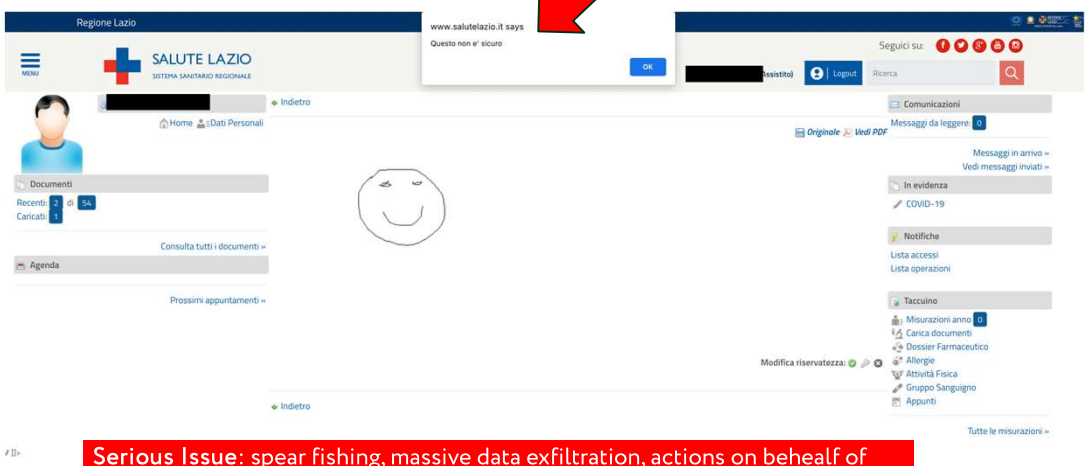
16

FSE – User Data



17

FSE – (distributed) Stored XSS



Serious Issue: spear fishing, massive data exfiltration, actions on behealf of the doctos, account takeover by password change?

18

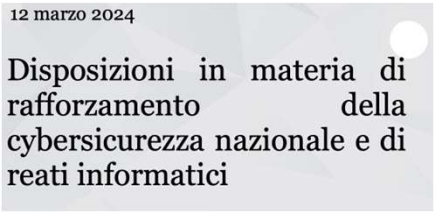
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Aftermath

Responsible disclosure → Notification about a fix

June 20, 2023 — 7+ months — January 26, 2024

- **7 months vs 15 days** for "decisive interventions" (recent cybersecurity bill) – 12 march 2024
- Closed case? two major remaining concerns on our side
  - What about the 19 remaining ITA regions? All unaffected?
  - Is the fix robust?



12 marzo 2024

Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

In dettaglio, il **comma 1** prevede che l'Agenzia per la cybersicurezza nazionale (ACN) possa segnalare, ad una serie di soggetti pubblici o che forniscono servizi pubblici, **specifiche vulnerabilità cui essi risultano potenzialmente esposti**; inoltre prevede che i destinatari di tali segnalazioni devono provvedere senza ritardo, e comunque non oltre **15 giorni** dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia.

Lorenzo Bracci

19

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Discussion & Suggestions

20

20

Suggestions

1. Use recognissance tools to do active monitoring

21

List of items purchased by Public Administration

oggetto_gara	oggetto_principale_contratto	importo_complessivo_gara	data_pubblicazione	data_scadenza_offerta	cf_amministrazione_appaltante	denominazione_amministrazione_appaltante
LAVORI DI SOMMA URGENZA RISANAMENTO CONSERVATIVO E RIMODULAZ	LAVORI	198879.0	27/09/2018	27/09/2018	2855540799	AZIENDA SANITARIA PROVINCIALE DI CATANZARO
ACQUISTO FARMACO MODITE DEPOT DITTA BRISTOL MYERS SQUIBB SRL	FORNITURE	7210.0	25/09/2018	09/10/2018	96024110635	ASL NAPOLI 2 NORD
ACQUISTO MONITOR	FORNITURE	200.0	28/09/2018	28/09/2018	763810587	FONDAZIONE ENASARCO
ADESIONE GARA REGIONALE DPI 2^ EDIZIONE LOTTO 5 OCCHIALI AD ASTINE	FORNITURE	6534.0	20/09/2018	20/09/2018	962520110	AZIENDA UNITA SANITARIA LOCALE N. 5 SPEZZINO
AFFIDAMENTO FORNITURA PRODOTTI DI PULIZIA PER LASILO NIDO COMUN	FORNITURE	1000.0	14/09/2018	29/09/2018	82795827	COMUNE LERCARA FRIDDI
NOLEGGIO QUADRIENNALE DI VEICOLI SENZA CONDUCENTE DA ASSEGNARE	FORNITURE	34392.0	27/09/2018	27/09/2018	2253930156	COMUNE DI SESTO SAN GIOVANNI
STAGE A DUBLINO 18-19	SERVIZI	121500.0	20/09/2018	22/10/2018	97020800153	ISTITUTO TECNICO STATALE PER IL TURISMO ARTEMISIA GENTILESCHI
PROCEDURA RISTRETTA PER LA FORNITURA DI DEFLUSSORI - REGOLATORI D	FORNITURE	577400.0	07/09/2018	09/08/2021	2101050546	AZIENDA OSPEDALIERA DI PERUGIA SANTA MARIA DELLA MISERICORDIA
MANUTENZIONE HARDWARE IBM SEDE CENTRALE (GARANZIA SUL SERVIZIO	SERVIZI	112000.0	17/09/2018	02/10/2018	80054330586	CONSIGLIO NAZIONALE DELLE RICERCHE
SERVIZI DI BUSINESS INFORMATION PER LA VALUTAZIONE DELLA POSIZIONE	SERVIZI	250000.0	10/09/2018	17/09/2018	6377691008	ENEL ITALIA SPA
SERVIZIO DI PULIZIA ORDINARIA C/O LOCALI E LORO PERTINENZE	SERVIZI	81402.0	14/09/2018	24/09/2018	193460680	COMUNE DI MONTESILVANO
PIANO DI INTERVENTO TRIENNALE DI NOLEGGIO MEZZI OPERATIVI PER LA M	SERVIZI	300000.0	27/09/2018	21/11/2018	1907990012	CITTA METROPOLITANA DI TORINO
FORNITURA DI DISPOSITIVI PER STOMIE CATETERI SONDE VESCICALI E ALTRI	FORNITURE	159158.68	11/09/2018	11/09/2018	1681590891	AZIENDA SANITARIA PROVINCIALE DI SIRACUSA
VIAG						
AFFI						
MAN						SPA
DAS						
CIG A						
ACCO						S BERICA
PROC						
ENERGIA ELETTRICA	SERVIZI	670.32	14/09/2018	17/09/2018	5175700482	ACQUE S.P.A.
FORNITURA PIATTAFORMA TECNOLOGIA GESTIONE PROCREAZIONE MEDICA	FORNITURE	140000.0	21/09/2018	21/09/2018	6485540485	ESTAR (ENTE DI SUPPORTO TECN
ACQUISIZIONE DI SERVIZI SUPPLEMENTARI RELATIVI AL CONTRATTO DI AFFI	SERVIZI	90159.6	13/09/2018	13/09/2018	1199250158	COMUNE DI MILANO
POMPA GRUNDFOS - ORD. 67.10512	FORNITURE	736.5	06/09/2018	07/09/2018	1763190509	ACQUE SERVIZI S.R.L.
PRODUZIONE CULTURALE NELLA FATTISPECIE DELLA REALIZZAZIONE DEL LU	SERVIZI	121000.0	08/09/2018	08/09/2018	93055550771	FONDAZIONE DI PARTECIPAZIONI

	Struttura	Acquisto	Dispositivo
1.	UNITA SANITARIA LOCALE ROMA	MANUTENZIONE ED ASSISTENZA TECNICA ANGIOGRAFO INNOVA 2000 01/012014-30/04/2014	innova 2000 firmware

AUTORITÀ NAZIONALE ANTICORRUZIONE

+

CVEs of medical devices

1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** GE Healthcare
- **Equipment:** GE Imaging and Ultrasound Products
- **Vulnerabilities:** Unprotected Transport of Credentials, Exposure of Sensitive System Information to an Unauthorized Control Sphere

Maps of purchases of vulnerable medical devices

https://www.nature.com/articles/s41598-023-45927-1

22

Suggestions

1. Use recognissance tools to do active monitoring
2. Move from a prescriptive to supportive approach

Do not dump the cyber sec problem on healthcare facilities

Suggestions

1. Use recognissance tools to do active monitoring
2. Move from a prescriptive to supportive approach
3. Use the community: bug bounty, open policies for bug reporting ecc.

25

Best Practice: Doctolib (300k HCPs)

Scope

In scope

- ✓ Doctolib public-facing websites:
  www.doctolib.fr www.doctolib.de www.doctolib.it
- ✓ Doctolib web application for professionals:
  pro.doctolib.fr pro.doctolib.de pro.doctolib.it
- ✓ Doctolib B2B website:
  info.doctolib.fr info.doctolib.de info.doctolib.it
- ✓ Doctolib API gateway:
  api.doctolib.fr api.doctolib.de api.doctolib.it
- ✓ Doctolib public infrastructure:
  *.doctolib.(fr|de|it|com|net)
- ✓ Doctolib iOS App:
  https://apps.apple.com/fr/app/doctolib/id925339063
- ✓ Doctolib Android App:
  https://play.google.com/store/apps/details?id=fr.doctolib.www&hl=fr

26

Best Practice - WHO

27

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

cnit

Lorenzo Bracciale

28