WORKSHOP GARR 2026

NET MAKERS

Organizzare un pentest studentesco (e sopravvivere)

Alvise Rabitti

Università Ca’ Foscari Venezia

talk outline

Introduzione

Cose fatte prima

Il pentest

Cose fatte dopo

Takeaways

pentest – cos’è?

[…] è un **attacco informatico** simulato autorizzato su un sistema informatico o una rete, eseguito **per valutare la protezione del sistema**.

Wikipedia

pentest – cos’è?

[…] è un **attacco informatico** simulato autorizzato su un sistema informatico o una rete, eseguito **per valutare la protezione del sistema**.

Wikipedia



Un vulnerability assessment è il processo di identificazione, valutazione e prioritizzazione delle vulnerabilità di un sistema

Wikipedia

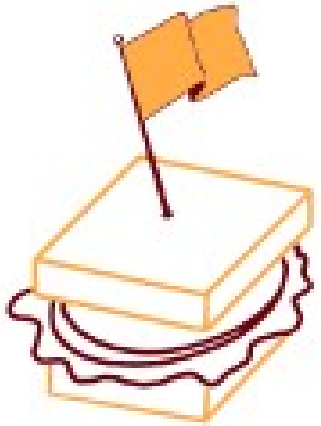
pentest - NIS2

il penetration testing è tra le misure minime che tutti i soggetti devono adottare nell'ambito della Gestione delle vulnerabilità e delle Politiche per valutare l'efficacia della gestione dei rischi

frequenza almeno annuale per l'infrastruttura perimetrale, le applicazioni esposte sul web e i sistemi critici.

insider threat

CYBER CHALLENGE.IT



BHACKARI

burocrazia

Referente “esterno”: docente di cybersecurity, che ha individuato 3 ragazzi (2 borse di ricerca + 1 tirocinio pagato)

Attività pagata e contrattualizzata con apposito documento

Referenti interni: Direttore Ufficio Sistemi e Infrastrutture, Responsabile per la Sicurezza Informatica

threat model / perimetro

Attaccante “normale”:
abile, ma senza particolari risorse di calcolo

Punti di accesso:
- Internet;
- la rete VPN fornita dall’Ateneo con profilo “biblio”;
- la rete wifi “eduroam” (attraverso uno degli Access Point di Ateneo);
- un host nella sottorete del Dipartimento di Informatica;
- un host nella sottorete in uso al personale di Ateneo.

threat model / perimetro

Nello spirito di una simulazione realistica e omnicomprensiva, il test può prendere in considerazione qualunque aspetto dei sistemi di Ateneo, ma viene richiesta, in particolare, l'analisi dei seguenti sistemi:

- servizi web al pubblico;
- dominio Active Domain utilizzato dai sistemi Windows di Ateneo.

proteggiamo lo studente

[...] **È possibile che queste attività causino l'indisponibilità o l'inconsistenza dei sistemi.**

[...] **Lo Studente si impegna a ridurre al minimo i predetti rischi ai sistemi, coordinandosi preventivamente con il personale dell'ASIT**

[...] **L'Ateneo si impegna a non rivalersi per eventuali danni subiti dai sistemi informativi**



proteggiamo l'organizzazione

Durante l'attività di penetration testing **lo Studente potrebbe venire a conoscenza di informazioni riservate che riguardano i sistemi e le reti dell'Ateneo, e i dati (anche personali) in essi contenuti** o da essi trattati. Lo Studente si impegna ad accedere solamente ai dati necessari per adempiere ai compiti affidati. Lo Studente si impegna a mantenere riservate tali informazioni, **condividendole esclusivamente con gli altri soggetti coinvolti nell'attività** ed individuati nella tabella A allegata, identificati tramite il loro account UNIVE.
Al fine di tutelare i dati dell'Ateneo in ogni fase del processo, lo Studente si impegna a **prestare la massima attenzione rispetto ai dati mantenuti in locale sui suoi sistemi**, e ad utilizzare per la loro **condivisione e discussione esclusivamente servizi della suite** Google Workspace (es. Google Drive, Google Chat) **messa a disposizione dall'Ateneo**. Qualora vengano rilevate delle situazioni di particolari gravità che possano causare particolari rischi per l'Ateneo, lo Studente dovrà avvisare immediatamente il referente dell'ASIT, la quale, nel caso siano coinvolti dati personali, provvederà a coinvolgere tempestivamente il Data Protection Officer (DPO) di Ateneo.
Il presente documento costituisce altresì nomina ad autorizzato al trattamento ai sensi dell'art. 29 del Regolamento 2016/679 e dell'art. 2 quaterdecies del D.Lgs. n. 196/2003, impartendo le necessarie istruzioni.
Al termine dell'attività di penetration testing, lo Studente si impegna a rimuovere dai suoi sistemi tutti i dati trattati, dandone conferma all'ASIT, e comunque a non divulgare a terzi informazioni e risultati derivanti dall'attività, a meno di esplicita autorizzazione.

proteggiamo l’organizzazione

Limiti chiari alla condivisione delle informazioni;

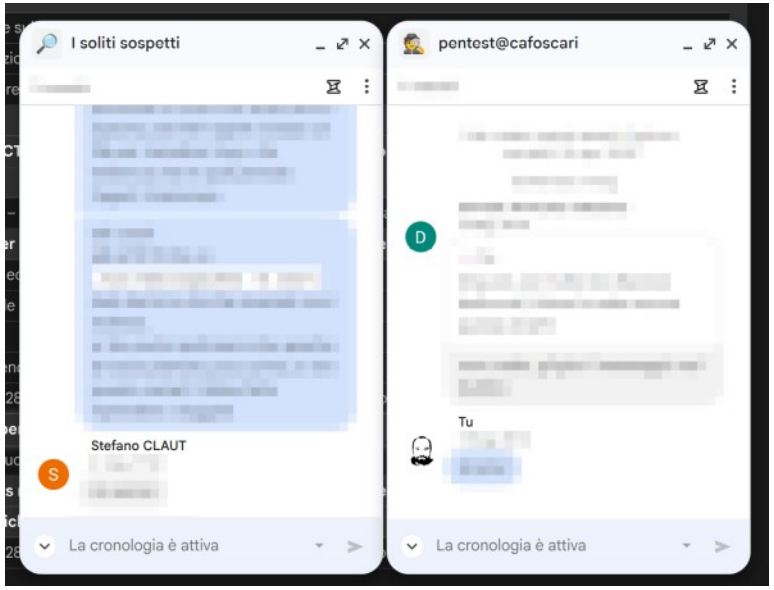
Limiti chiari agli strumenti da utilizzare per gestire le informazioni, forniti dall’Ateneo;

Nomina al trattamento;

Esplicito accordo di rimozione dei dati al termine dell’attività.

si parte!

2 chat



1 drive



difese


pentest@cafoscari
D
Non riesco più a connettermi a niente nel range ip di ateneo
La cronologia è attiva

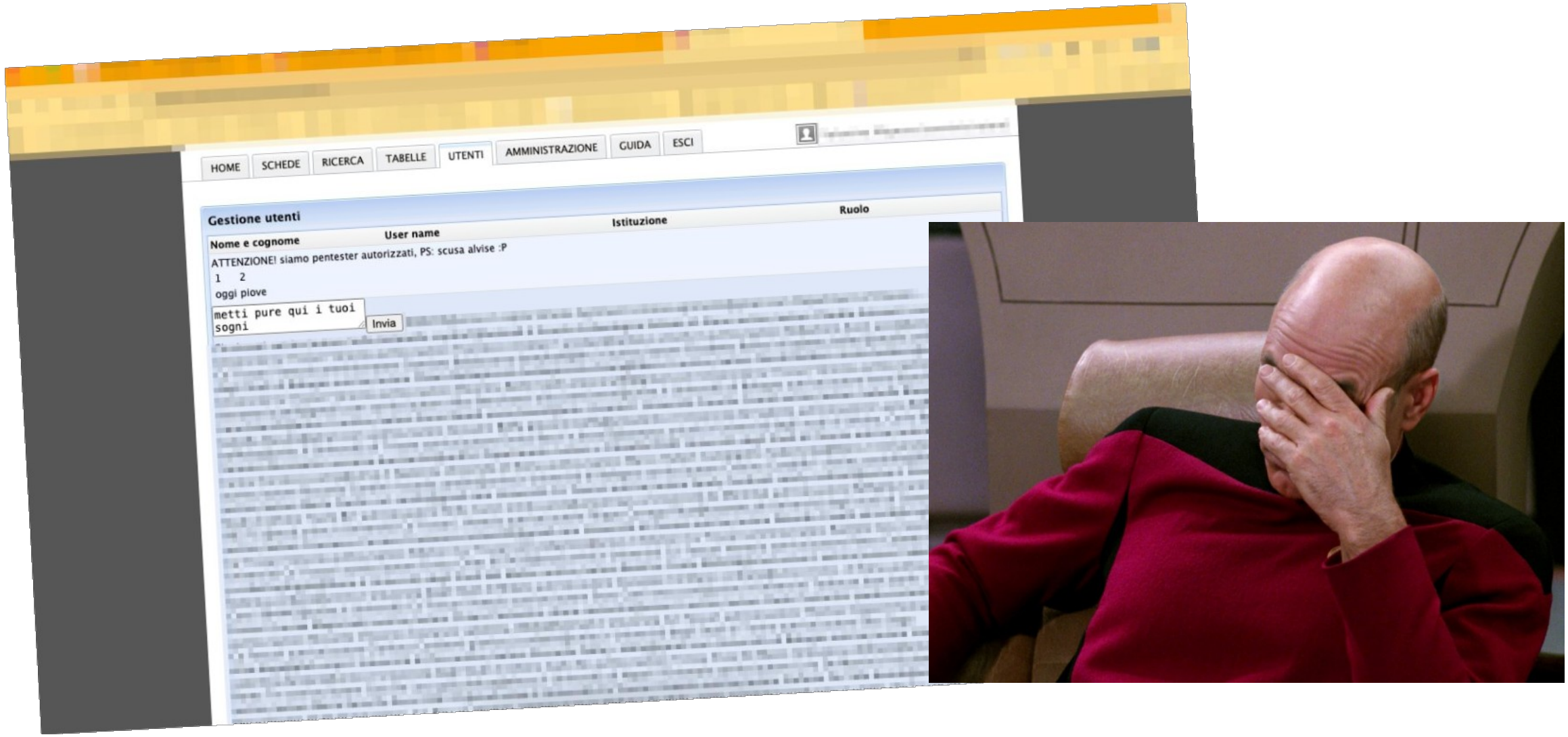

il WAF
Letteralmente qualsiasi webapp unive
SRGRAFO

qualche ritrovamento utile

un servizio “di appoggio” che poi era rimasto lì

XSS markup injection

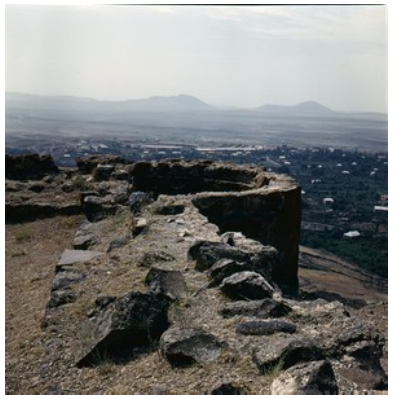
danni collaterali



altri ritrovamenti...

...misteriosi





...interessanti



fine!



fine giugno

1 settembre



Accordi



Report



Presentazione

takeaways

Esperienza positiva

I ragazzi… sono ragazzi, e quindi vanno un po’gestiti (in particolare nella priorità da esplorare)

Aumento del know how e della fiducia interna tra PTA/Docenti/Studenti

Non tutto il perimetro proposto è stato esplorato

takeaways

- Difese automatiche hanno funzionato
- Sono scattati pochi allarmi

...e quindi?

Fixiamo

Rivediamo gli indicatori di allarme

Rivediamo il perimetro

Ripetiamo!

GRAZIE!

Domande?

www.partici.fi
(codice 83995288)

alvise.rabitti@unive.it

WORKSHOP GARR 2026
NET MAKERS