Vulnerabilità informatiche (semplici)..

in infrastrutture complesse..

“..il contenuto di questo speech è di pura fantasia, ogni riferimento a infrastrutture reali o fatti realmente accaduti è puramente casuale”

Area Sicurezza, e-Academy

7 ottobre 06 - Smau - Milano

Italian Security Mailing List

SIKUREZZA.ORG

< free advertising

Relatore:

NETWORK enforcer SECURITY

Igor Falcomatà

Chief Technical Officer

ifalcomata@enforcer.it

about:

aka “koba@sikurezza.org”

- attività professionale:
  - analisi delle vulnerabilità e penetration testing
  - security consulting
  - formazione
- altro:
  - sikurezza.org
  - (Er|bz)lug

Relatore:

NETWORK enforcer SECURITY

Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it

Di cosa parleremo

per evitare di fare questo tipo di errori/dimenticante

- vulnerabilità semplici
  - errori di configurazione
  - disattenzioni
  - errori progettuali/concettuali
- ma difficili da rilevare
  - con tool VA automatizzati
- infrastrutture complesse
  - relazioni tra applicazioni e sistemi diversi

Esempio #1

portale web, accesso con credenziali (SSL)

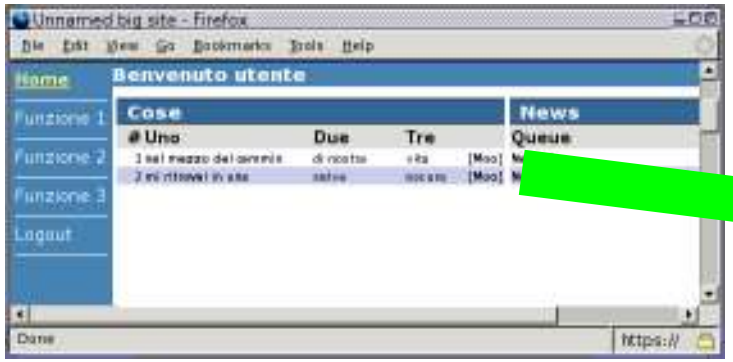
authcookie:

JKkhkaae09f2196aa88c8687

corretta gestione della sessione e dei privilegi per tutte le funzioni, tranne che ...

Esempio #1 - “Ops, il cookie...”

...una particolare funzione che utilizza un software esterno...



processa i dati ricevuti e crea un file di output in una directory, restituendo il link al nome del file

Risultati

Esempio #1 - “Ops, il cookie...”

/output/00112345.ext

- è possibile accedere a questa directory senza autenticazione:

~~JKkhkaac09f2196aa88c8687f~~

00112345 .. 6 .. 7 ..

/output/00112301.ext

[..]

/output/00112345.ext

- nome file predicibile (incrementale)
- directory browsabile
- file di precedenti elaborazioni non rimossi

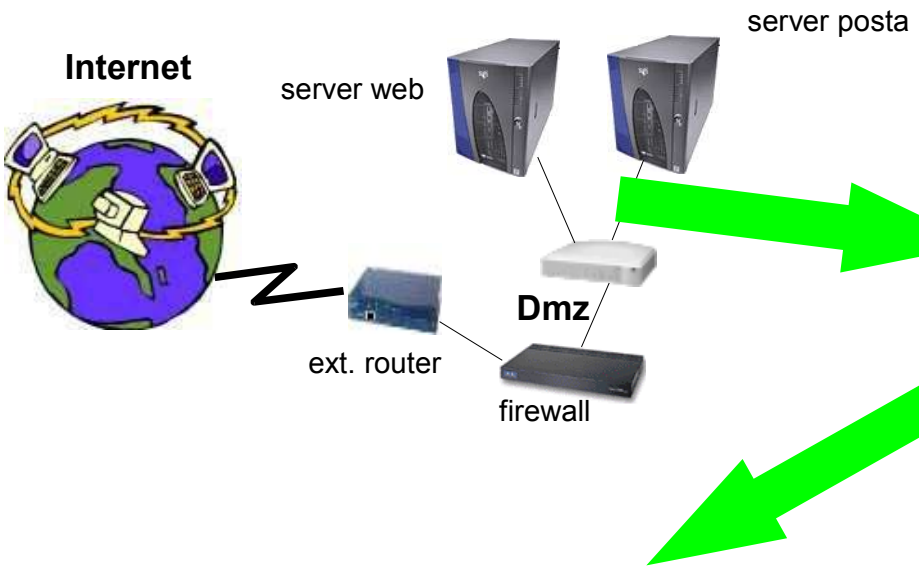
Sempre in tema...

OWASP Top Ten: Broken Authentication and Session Management

- integrazione errata tra sistemi di SSO e cookie/sessioni gestite dalle singole applicazioni
    - il cookie del sistema di SSO viene verificato solo durante la fase di login nell'applicazione, modificandolo dopo si può fare role escalation
- modifica dei cookies
    - non cifrati
    - cifrati ma senza verifica dell'integrità
- accesso a sezioni “nascoste” (OWASP: Broken ACL)
    - /old/ /new/ /backup/ /login.old

Esempio #2

analisi perimentrale da remoto



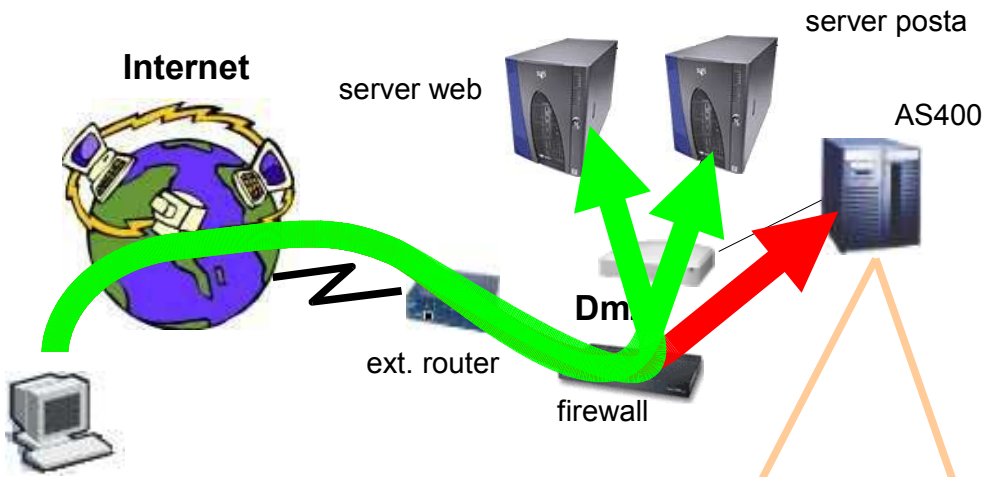
mappatura dei sistemi/servizi raggiungibili pubblicamente

le politiche di filtro ed il firewall sono correttamente configurati;

vengono esposti solamente i servizi necessari, tranne...

Esempio #2 - “tn32che?”

...una porta telnet-ssl



che utilizzando un apposito client tn3270 presenta una schermata di login di un AS400

Esempio #2 - “tn32che?”

bruteforcing utenze

password

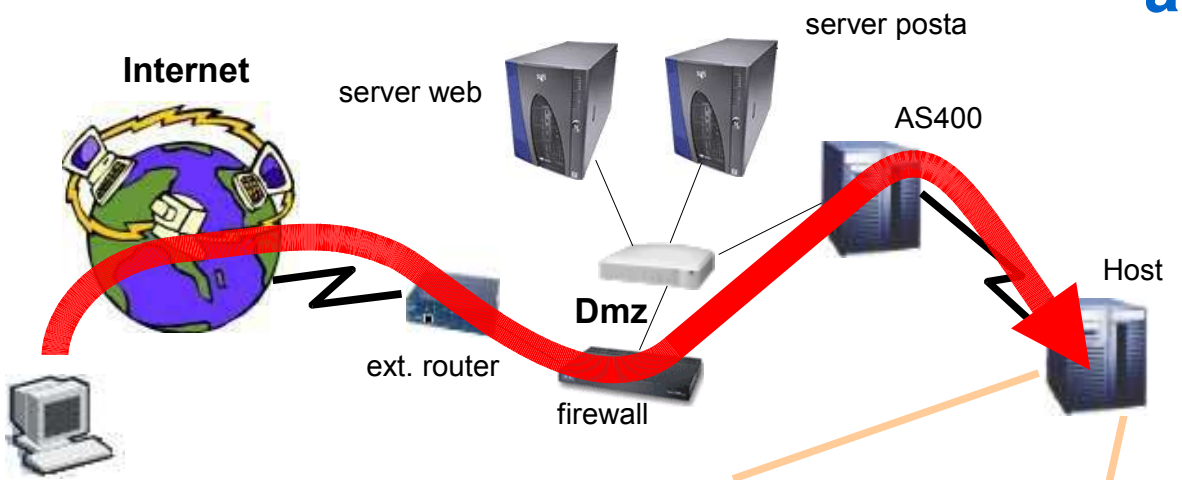
- **account di default**
- **account generici**
- **nomi di potenziali utenti identificati tramite analisi del sito**

è stata identificata una credenziale di accesso valida:

utente “qualcosa”, password uguale...

Esempio #2 - “tn32che?”

e, una volta entrati nel sistema, la possibilità di collegarsi ad un altro AS400 remoto via WAN



con una nuova schermata di login...

Esempio #2 - “tn32che?”

le credenziali valide sull'altra macchina, qui non sono valide ma...

...è possibile entrare con un'utenza di sistema con password banale

ed avere accesso ad informazioni particolarmente rilevanti, con la possibilità di modificarle...

Esempio #2bis - “Telefono/Lan”

- centralino telefonico
  - accesso al modem integrato per teleassistenza attraverso chiamata telefonica, selezionando l'interno di default
  - login con credenziali specifiche (senza password)
  - sistema unix “legacy”
  - cat /etc/passwd
  - bruteforcing password root
  - accesso completo al sistema...
  - ...collegato in LAN

Sempre in tema...

spesso è sufficiente un singolo servizio esposto

- remote admin
  - telnet, ssh, rdesktop, vnc, pcanywhere, snmp, ...
  - interfacce web (pannelli vari, appl. specifiche, ...)
- accesso a filesystem
  - cifs, nfs, ftp/sftp, dav, web based, ...
- accesso a database
  - porte db esposte
  - interfacce web

Sempre in tema...

ma si trovano anche workstation e server

- **workstation**
  - **“ho messo la mia stazione direttamente su Internet, perché mi è più comodo; ma solo la mia, eh...” (admin)**
  - **“il software di remote-banking ha problemi con il proxy, perché non lo mettiamo fuori?” (admin)**
- **server**
  - **server di test**
  - **server “non più” in produzione**
  - **server dimenticati ...**

Sempre in tema...

o maniere vecchie e nuove per superare i controlli perimentrali

- modem, RAS & co.
- wireless
- WAN, linee dedicate con partner, fornitori, ...
- accesso fisico alla struttura o ai cablaggi
- X25 (perché, esiste ancora?)

Esempio #3

- analisi di sicurezza di un sistema “embedded” basato su Win* e della relativa infrastruttura ed implementazione
- case blindato (mmm, a cosa servirà?)
- WAN privata
- funzionalità (ristrette) di web browsing

Esempio #3

- **MitM della sessione HTTPS**
- **“accetti il certificato della CA non riconosciuta?”**
  - **(touchscreen) click -> SI**
- **pagina contenente malicious code**
- **MitM della sessione HTTPS**
- **“vuoi eseguire bo2k.exe?”**
  - **(touchscreen) click -> SI**

Sempre in tema...

- sistemi embedded
  - apparecchiature di rilevamento presenze
  - apparecchiature per controllo accessi
  - videosorveglianza
  - controllo ambientale
- e meno embedded
  - spesso basati (almeno la componente di management e registrazione) su os standard
  - con vulnerabilità standard
  - accessibili dalla LAN

Esempio #4

Gioco a premi “on-line”

un file SWF (Flash) viene fornito all'utente (ed eseguito in locale)

i risultati della partita vengono inviati al server attraverso un POST

i parametri non sono intelleggibili

POST https://sito/url HTTP/1.0

param=amn398asjfg334

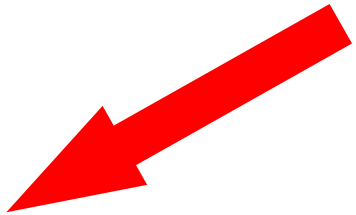
l'immagine è tratta da Frozen Bubble: http://www.frozen-bubble.org/

Esempio #4 – “hey, ho vinto!”

POST https://sito/url HTTP/1.0

param=amn398asjfg334

- anche se il parametro di ritorno non è interpretabile “a vista”
- modificandolo a caso è possibile capirne la struttura
- non vi è un meccanismo di controllo dell'integrità
- è possibile barare, modificando il parametro che corrisponde al punteggio



POST https://sito/url HTTP/1.0

param=amn398jazwl334

Sempre in tema...

- invia il codice e vinci
  - codici che non vengono annullati
  - generazione di codici (random o mirata)
- mobile code (flash, java, etc.)
  - modifica del traffico
  - modifica del timer della stazione locale
  - reverse engineering

Esempio #5

form di login

password:

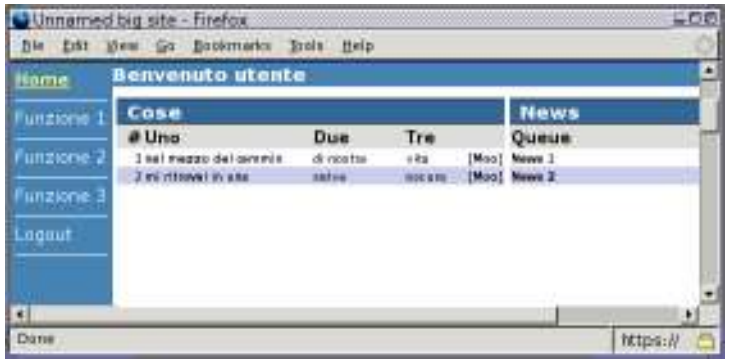
' or 'a'='a

select * from utenti where userid = 'utente' and

password = '' or 'a'='a'

Esempio #5 – good ole sql injection

accesso senza credenziali



anche se siamo nel 2006, non scommetterei sull'estinzione delle form(e) di login vulnerabili a questo tipo di attacco...

select * from utenti where userid = ? and password = ?

execute(query, param1, param2)

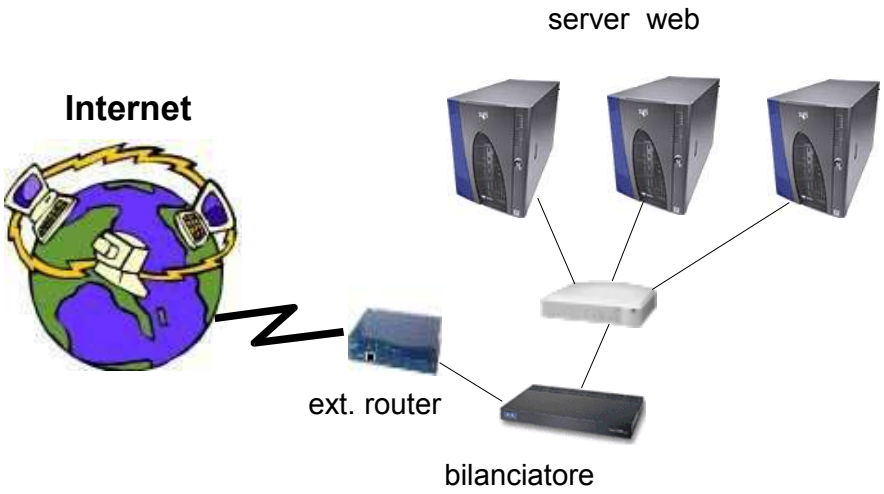
Sempre in tema...

OWASP Top Ten: Input validation

- le problematiche di input validation sono ancora molto diffuse, sia nelle applicazioni web
  - in particolar modo nelle sezioni accessibili solo con credenziali
  - in tutti quei casi in cui la manipolazione non sia diretta
- che nelle applicazioni tradizionali

Esempio #6

pool web server



richieste smistate su server "gemelli" per bilanciare il carico (oltre ad HA)

cosa succede se una o più macchine del cluster sono configurate in maniera differente?

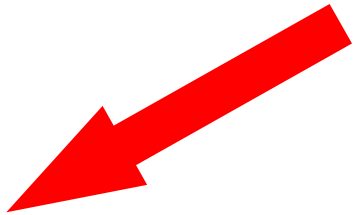
Esempio #6 – “sbilanciamoci”

PUT http://sito/exc.asp HTTP/1.0

-> 405 Not Allowed

[..]

- può capitare che, avendo a che fare con pool di server dietro a bilanciatore/i...
- che alcuni sistemi siano configurati/aggiornati diversamente



PUT http://sito/exc.asp HTTP/1.0

-> 200 Bingo

[..]

- con vulnerabilità specifiche

Esempio #7

portale web, accesso con credenziali (SSL)

username: demo

password: demo

"salve, professor Falken"

Domande?

(grazie per l'attenzione)

Area Sicurezza, e-Academy

7 ottobre 06 - Smau - Milano

Italian Security Mailing List

SIKUREZZA.ORG

< free advertising

Relatore: Igor Falcomatà
koba@sikurezza.org