



Consideratii privind securitatea aplicatiilor Web

Sabin-Corneliu Buraga

Facultatea de Informatica

Universitatea "A.I.Cuza" din Iasi, Romania

<http://www.infoiasi.ro/~busaco/>



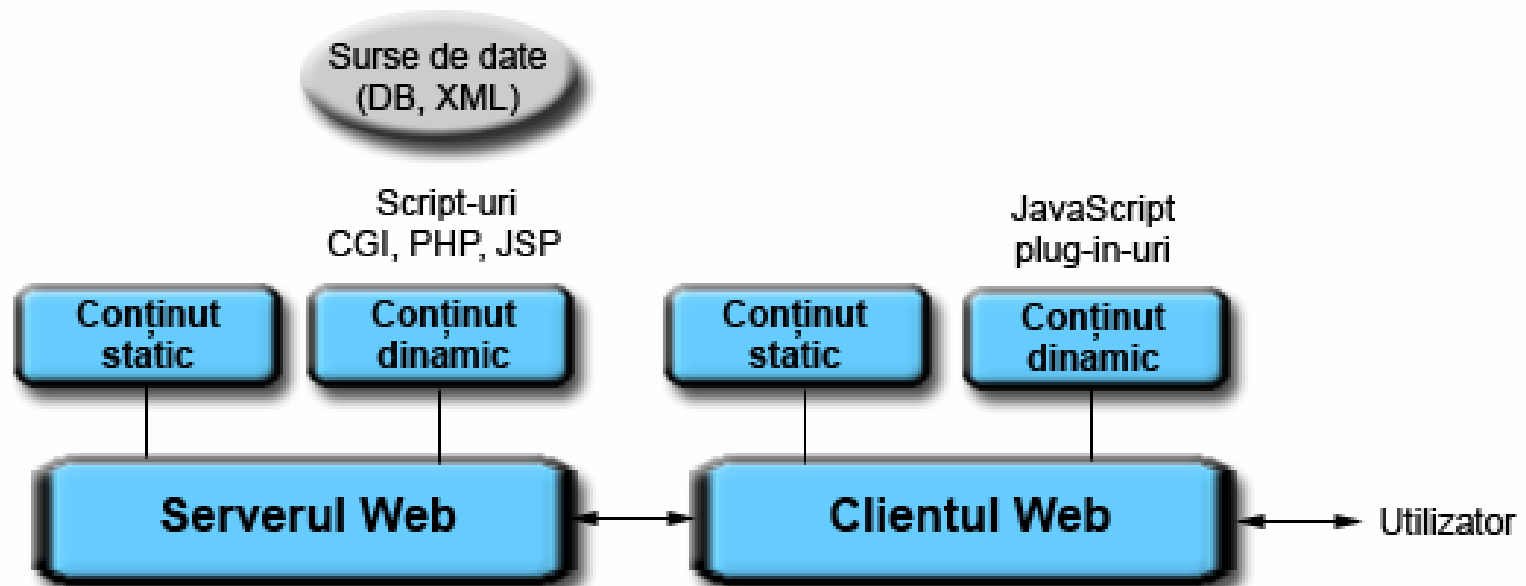
cuprins

- Preliminarii
- Tipuri de atacuri
- Prevenirea & supravietuirea
- Monitorizarea & testarea
- Aspecte importante



preliminariii

- Arhitectura generala a unui sit Web dinamic (aplicatie Web) – detalii in (Buraga, 2003; Buraga, 2005)





preliminariii

- **Incident de securitate** \equiv eveniment aparut in cadrul retelei, cu implicatii asupra securitatii unui calculator sau a retelei
 - Provenind din **interiorul** ori **exteriorul** retelei
- Multe protocoale de baza ale Internetului (inclusiv HTTP) nu au luat in calcul vulnerabilitatile ce pot surveni
- ***Cracker*** vs. ***hacker***



preliminariii

- **Vulnerabilitate** \equiv slabiciune a unui sistem hardware/software ce permite utilizatorilor neautorizati sa aiba acces asupra sa
- **Nici un sistem nu este 100% sigur**
- Vulnerabilitatile apar si datorita proastei administrari



preliminariii

- Cauzele existentei vulnerabilitatilor (Acostachioaie, 2003)
 - *Bug*-uri (erori) existente in programe (scripturi, servere Web, navigatoare,...), introduse deseori neintentionat
 - Ignorarea/nedocumentarea *bug*-urilor existente (cunoscute)
 - Configurarea necorespunzatoare a programelor, serverelor si retelelor
 - Lipsa suportului din partea producatorilor
 - Comoditatea sau necunoasterea problemelor de securitate de catre administrator ori de conducerea organizatiei



atacuri

- Cunoasterea profilului atacatorului
- Atribute ce trebuie considerate:
 - Resursele disponibile
(financiare, tehnice,... + pregatirea in domeniu)
 - Timpul alocat
(atacatorii rabdatori vor avea mai mult succes)
 - Riscul asumat – depinde de obiective
(atacul ar putea fi revendicat sau nu de *cracker*)
 - Accesul la Internet si calitatea acestuia: tip (*dial-up*, conex. satelit,...), mod de alocare a IP-ului etc.
 - Obiectivele urmarite (e.g., recunoastere mondiala, denigrarea tinteii, furt de informatii, furt de bani)



atacuri

- Tipuri de atac
 - Accesul utilizator
 - Atac prin acces via cont-utilizator obisnuit sau cu privilegii superioare
 - Etape:
 - Colectarea de informatii – utilizatori, vulnerabilitati,...
 - Exploatarea
 - Deteriorarea
 - » Modificare de informatii
 - » Acces la date importante
 - » Asigurarea accesului ulterior la sistem
 - » Modificarea jurnalelor de sistem



atacuri

- Tipuri de atac
 - Accesul de la distanta
 - Nu necesita acces-utilizator la sistem
 - Creaza refuzuri de servicii prin cereri incorecte ori “in rafala” – **DOS (Denial of Service)**, **DDOS (Distributed DOS)**
 - Efecte:
 - Distrugerea unui server ori unei aplicatii Web
 - Defectarea/incetinirea (temporara) a serverului Web sau a sistemului



atacuri

- Tipuri de atac
 - Accesul de la distanta la diverse aplicatii
 - Trimitere de date invalide aplicatiilor, nu serviciilor de retea (traficul nu e afectat); e.g., **SQL injection** sau **Cross-Site Scripting**
 - Nu necesita obtinerea de acces utilizator
 - Etape:
 - Colectarea de informatii – identificarea aplicatiei (e.g. server sau client Web, aplicatie Web)
 - Exploatarea – trimiterea continutului, direct sau indirect, spre aplicatie
 - Deteriorarea



atacuri

- Tipuri de atac
 - Accesul de la distanta la diverse aplicatii
 - **SQL injection**
 - Scrierea unor interogari SQL ce permit afisarea, alterarea, stergerea de date din bazele de date via formulare Web ori direct in URI
 - **Cross-Site Scripting (XSS)**
 - “Injectarea” in cadrul sistemului, pt. executia direct in browser, a scripturilor JavaScript/VBScript
 - Exemplu: `` care redirectioneaza utilizatorul spre alt sit ori blocheaza navigatorul
 - Detalii in (Long, 2005)



atacuri

- Tipuri de atac
 - Inocularea de programe pe calculatorul utilizatorului
 - Plasarea de programe *malware* (virusi, spioni, cai troieni, bombe,...) via *script*-uri, *plugin*-uri, componente ActiveX etc.
 - Efecte:
 - Apelarea neautorizata de programe
 - Colectarea/distrugerea de resurse
 - Lansarea de atacuri spre alte sisteme
 - Crearea de usi ascunde (*traps*, *backdoors*)
 - Si altele...



atacuri

- Tinta
 - Organizatii publice sau guvernamentale
 - Recunoastere in rindul *cracker*-ilor
 - Captarea atentiei mass-mediei
 - Revendicari etice, politice,...
 - Furnizori de servicii Internet
 - Sabotarea activitatii
 - Companii private
 - Discreditare
 - Furt de informatii
 - Razbunare din partea fostilor angajati
 - Persoane fizice
 - Cu scop recreational



atacuri

- Detectarea posibilelor vulnerabilitati (datorate unor configuratii incorecte ori implicite ale serverelor si/sau aplicatiilor Web) se poate realiza apelind la un motor de cautare



atacuri

- Exemple de actiuni – vezi (Buraga, 2005):
 - Detectia versiunilor de programe avind *bug*-uri cunoscute: “[Apache/2.0.52 server at](#)”
 - Accesul la fisiere *.bak*: [inurl:index.php.bak](#)
 - Accesarea intranet-ului: [intitle:intranet](#)
 - “Vinarea” de e-mail-uri:
[“@gmail.com” –www.gmail.com](#)
 - Detectarea paginilor de administrare: “[admin login](#)”
 - Gasirea unor instalari implicite:
[intitle:“welcome to” intitle:internet IIS](#)
 - Localizarea interfetelor spre sistemele de baze de date: [inurl:main.php phpMyAdmin](#)



prevenirea

- La ce nivel trebuie luate masuri de securitate?
 - Nivelul fizic: inhibarea ascultarii mediilor de transmisie, interzicerea accesului fizic la server,...
 - Nivelul legatura de date: criptarea legaturii
 - Nivelul retea: ziduri de protectie (*firewall*-uri)
 - Nivelul transport: criptarea conexiunilor (**SSL – Secure Socket Layer, TLS – Transport Layer Security**)
 - Nivelul aplicatie: monitorizarea & actualizarea programelor (sistem de operare, server Web, server de aplicatii, biblioteci,...), jurnalizarea accesului, educarea utilizatorilor, adoptarea de politici generale de securitate



prevenirea

- Elaborarea de politici de securitate (Garfinkel & Spafford, 2001)
 - Planificarea cerintelor de securitate
 - Confidentialitate, integritate, disponibilitate, control al accesului
 - Evidentierea riscurilor
 - Scenarii de risc (“Cine decide care date sint importante?”, “Cit de critice sint datele?”, “Care e perioada in care situl nu va fi operational?”)

Masurile luate pot fi tehnice si non-tehnice.



prevenirea

- Elaborarea de politici de securitate (cont.)
 - Analiza raportului cost-beneficii
 - Costurile prevenirii, refacerii dupa dezastru etc.
 - Stabilirea politicilor de securitate
 - Politica generala (nationala, organizationala,...)
 - Politici separate pentru diverse domenii protejate
 - Standarde & reglementari (recomandari)

Masurile luate pot fi tehnice si non-tehnice.



prevenirea

- De retinut!
 - Atacatorul poate alege cel mai slab punct al sistemului (siguranta sistemului este data de cea a celui mai vulnerabil aspect al acestuia)
 - Ne putem apara doar contra atacurilor cunoscute, dar atacatorul poate exploata vulnerabilitati misterioase
 - *Cracker*-i pot atasa oricind, vigilenta trebuie sa fie permanenta
 - Atacatorul nu tine cont de legi, reguli, recomandari ori de bunul-simt



prevenirea

- Elaborarea de politici de securitate – exemplu
 - Gestionarea accesului (nume de cont, alegerea si stabilirea unei reguli de schimbare a parolelor)
 - Clasificarea utilizatorilor (grupuri, permisiuni, utilizatori speciali, utilizatori administratori,...) – constituirea **ACL (Access Control List)**
 - Accesul la resurse si modul de exploatare a sitului
 - Monitorizarea activitatii (fisiere de jurnalizare)
 - Administrarea copiilor de siguranta (tipuri de salvari, medii de stocare, durata pastrarii,...)



supravietuirea

- **Supravietuirea** \equiv capacitatea unui sistem (calculator/retea) de a-și îndeplini misiunea, în timp util, în pofida atacurilor, defectelor sau accidentelor
- **Atac** \equiv eveniment potential distrugator provocat intentionat de persoane rau-voitoare
- **Defect** \equiv eveniment potential distrugator cauzat de deficiente ale sistemului sau ale unui factor de care depinde sistemul (e.g. defecte hardware, *bug*-uri software, erori ale utilizatorilor)
- **Accident** \equiv evenimente aleatoare (neprevăzute); exemple: dezastre naturale sau căderi de tensiune



supravietuirea

- Sistemul trebuie sa-si duca pina la capat misiunea chiar daca unele componente sau parti din sistem sint afectate ori scoase din uz
- Sistemul trebuie sa sustina macar indeplinirea **functiilor vitale** (*mission-critical*)
 - Identificarea serviciilor esentiale (e.g., acces la lista produselor)
- Proprietati ale sistemului:
 - **Rezistenta la atacuri** ≡ strategii de respingere a atacului (i.e. validarea obligatorie a datelor, autentificarea utilizatorilor, acordarea privilegiilor minime)
 - **Recunoasterea atacurilor si efectelor lor** ≡ strategii pentru restaurarea informatiilor, limitarea efectelor, mentinerea/restaurarea serviciilor compromise
 - **Adaptarea la atacuri** ≡ strategii pentru imbunatatirea nivelului (sansei) de supravietuire (invatarea din greseli)



monitorizare & testare

- Teste de verificare a:
 - Capacitatii de deservire a clientilor
 - Robustetei
 - Rularii in situatii extreme
- Instrumentele de stresare (*stressing tools*) pot da informatii privitoare la:
 - Performanta (timp de raspuns, timp de generare a continutului)
 - Scalabilitate (memorie ocupata, utilizarea discului, nr. inreg. inserate,...)
 - Corectitudine
(functionarea eronata a unor componente)



monitorizare & testare

- Metodologii de analiza a riscurilor:
 - **DREAD** (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability)
 - **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
 - **STRIDE** (Spoofing identity, Tempering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege)
 - **OSSTMM** (Open Source Security Testing Methodology Manual)

www.osstmm.org



aspecte importante

- Securitatea unei aplicatii Web:
 - Trebuie sa ia in considerare **arhitectura**, **logica**, **codul-sursa** si **continutul** in ansamblu
 - Nu vizeaza vulnerabilitatile sistemului de operare ori ale programelor auxiliare
- Vulnerabilitatile unui sit nu sint “celebre” si vor fi independente deseori de securitatea sistemului pe care e exploatat situl



aspecte importante

- Tipuri de vulnerabilitati specifice (Buraga, 2005; Garfinfel & Spafford, 2001):
 - Probleme de autentificare
 - Managementul sesiunilor
 - Injectarea de scripturi (XSS) ori comenzi SQL
 - Expunerea (involuntara) a informatiilor delicate (*information disclosure*)
 - Accesul la codul-sursa ori la fisierele de configurare a aplicatiei Web



aspecte importante

- Riscurile de securitate nu vizeaza numai proprietarul sitului, ci si utilizatorul final
- Disconforturi cauzate de un sit nesigur:
 - Financiare (pierdere de bani/informatii)
 - De performanta
(blocarea navigatorului, incetinirea actiunilor,...)
 - Psihologice (insatisfactie)
 - Sociale (lipsa comunicarii, sincrone sau nu, cu partenerii de munca/afaceri)
 - De timp
(navigare greoaie, deturnare spre alt sit,...)



referinte

- D. Acostachioaie, *Securitatea sistemelor Linux*, Polirom, Iasi, 2003
- S. Buraga, *Proiectarea siturilor Web* (editia a doua), Polirom, Iasi, 2005: <http://www.infoiasi.ro/~design>
- S. Buraga (coord.), *Aplicatii Web la cheie*, Polirom, Iasi, 2003: <http://www.infoiasi.ro/~phpapps>
- S. Garfinkel, G. Spafford, *Web Security, Privacy and Commerce*, O'Reilly, 2001
- J. Long, *Google Hacking for Penetration Testers*, Syngress Publishing, 2005



rezumat

- Preliminarii
- Tipuri de atacuri
- Prevenirea & supraviețuirea
- Monitorizarea & testarea
- Aspecte importante



Mulumiri pentru atentie! Intrebari...?