On Security of Web Applications

Dr. Sabin-Corneliu BURAGA
Faculty of Computer Science, "A.I.Cuza" University of Iaşi, România
busaco@infoiasi.ro, http://www.infoiasi.ro/~busaco/

The paper presents main issues concerning the security of the actual Web applications and provides details about the possible security risks (e.g., SQL injection or Cross-Site Scripting) for the deployment of e-business Web sites. Also, the material describes different solutions to prevent or to survive to possible dangerous attacks.
Keywords: *Web Applications, Security, Treats, Solutions.*

Introducere

Web-ul – prin evoluția continuă a limbajelor bazate pe XML (*Extensible Markup Language*) – poate fi considerat un veritabil *sistem hipermedia distribuit*, utilizând ca infrastructură Internet-ul (Buraga, 2001; W3C, 2005). Prin popularea acestei infrastructuri cu seturi de componente orientate-obiect şi găsirea de modalități (semantice) de integrare a acestora, Web-ul poate fi privit ca un mediu eterogen pentru dezvoltarea şi exploatarea de sisteme obiectuale distribuite menite a manipula componente multimedia. Una dintre problemele importante pe care o discută acest articol este legată de securitatea generală a aplicațiilor şi siturilor Web. Se iau în considerație şi unele aspecte privitoare la riscurile de securitate şi la detectarea vulnerabilităților aplicațiilor *e-business*.

2. Arhitectura unei aplicații Web

Inițial, spațiul WWW era compus din pagini (documente) statice – incluzând text şi imagini, apoi elemente multimedia – interconectate prin intermediul legăturilor hipertext (Buraga, 2001; Buraga, 2005). Aplicații de tip client (precum navigatoarele Web) erau folosite pentru accesarea – via adrese (URI) – a reprezentării acestor resurse, stocate pe servere Web. Programe suplimentare (*plug-in*-uri), incluse în navigatoarele Web, erau menite să redea tipuri de conținuturi nestandardizate, ca fişiere Word, PostScript, *PDF* (*Portable Document Format*), Flash etc. Pentru a oferi conținut dinamic utilizatorilor, sunt adoptate diverse modalități programatice, reprezentate pe partea de server de programe *CGI* (*Common Gateway Interface*), servere de aplicații precum *PHP* (*PHP: Hypertext Processor*), *JSP* (*Java Server Pages*), *ASP* (*Active Server Pages*) sau ASP.NET, iar pe partea de client de programe JavaScript sau *applet*-uri Java.

De remarcat faptul că o serie de elemente programabile funcționează drept componente *middleware* (generând de fapt o arhitectură *3-tier* ori *N-tier*), reprezentând interfețe pentru accesarea unor servicii aflate la distanță (*e.g.*, sisteme relaționale de baze de date ori baze de date native XML).

Arhitectura generală a unei sit Web dinamic (aplicație Web) este prezentată în figura 1.

3. Asigurarea securității Web

3.1 Preliminarii

Un aspect important – dar care este neglijat, din păcate – este cel al asigurării securității sitului. Orice aplicație (în cazul nostru, sit) poate fi victima unui *incident de securitate*, i.e. a unui eveniment apărut în cadrul rețelei, cu implicații asupra securității, provenind din interiorul sau din exteriorul organizației. La momentul creării, multe protocoale Internet (prin care se numără şi protocolul HTTP) nu au luat în calcul posibilele vulnerabilități se pot surveni. *Vulnerabilitatea* se referă la slăbiciunea unui sistem hardware şi/sau software care permite utilizatorilor neautorizați să aibă acces asupra acestuia (Acostăchioaie, 2003). Nici un sistem informatic nu poate fi considerat 100% sigur, iar vulnerabilitățile pot apărea şi datorită unei inadecvate administrări.

3.2 Cauze ale vulnerabilităților

Principalele cauze ale existenței vulnerabilităților sunt (Acostăchioaie, 2003; Oprea,

2003):

• *bug*-urile (erorile) din cadrul programelor (*script*-uri, servere Web, navigatoare etc.), introduse deseori neintenționat;

• ignorarea şi/sau nedocumentarea *bug*-urilor deja existente (cunoscute);

• configurarea necorespunzătoare a programelor, serverelor şi rețelelor (de exemplu, o configurare precară a serverului Web poate conduce la accesarea unor fişiere ori baze de date conținând informații confidențiale, precum parole, coduri ale cărților de credit etc.);

• lipsa suportului din partea producătorilor de software;

comoditatea sau necunoaşterea problemelor de securitate de către administrator şi/sau factorii de conducere ai organizației (un aspect foarte important este cel al educării utilizatorilor, plecând de la vârful piramidei resurselor umane).

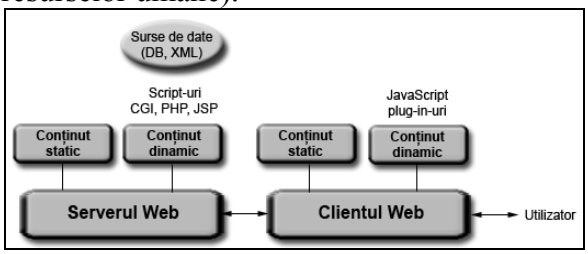

Fig.1. Arhitectura unei aplicații Web

3.3 Niveluri şi tipuri de atacuri

Nivelurile de atac pot varia de la unul oportunist (de exemplu, în scop „recreațional", fără obiective/ținte clar definite) la cel sofisticat (atacatorul are un obiectiv foarte bine conturat şi poate poseda cunoştințe tehnice avansate, măsurile de prevedere obişnuite nereprezentând un impediment).

Atacurile se pot încadra în următoarele tipuri (Acostăchioaie, 2003):

• accesul-utilizator – atacatorul realizează atacul via un cont de utilizator obişnuit sau având privilegii superioare (de exemplu, află sau ghiceşte parola unui vizitator şi client al unui sit de comerț electronic; dacă acel utilizator era şi administratorul sitului, atunci pagubele vor fi mult mai mari); acțiunile pe care le poate întreprinde un atacator în cazul în care a avut succes sunt cele de obținere a unor date importante, de alterare a acestora, de asigurare a accesului ulterior ori de modificare a unor parametri ai sistemului;

• accesul de la distanță – nu necesită accesutilizator la sistem, atacatorul încercând a realiza refuzuri de servicii (în cazul nostru, ale serverului Web) prin cereri incorecte ori prin trimiterea „în rafală" de solicitări – o astfel de tehnică se numeşte *DOS* (*Denial Of Service*), iar dacă atacurile sunt realizate simultan de pe mai multe maşini asistăm la apariția unui *DDOS* (*Distributed Denial Of Service*);

• accesul de la distanță la diverse aplicații – presupune şi trimiterea de date invalide aplicațiilor (Web), fără a necesita obținerea unui cont de utilizator. Două categorii principale de atacuri asupra siturilor Web sunt injectările de cod SQL (*SQL injection*) şi *XSS* (*Cross-Site Scripting*) – menționate în lucrări precum (Buraga, 2005), (Howard & LeBlanc, 2003) şi (Long, 2005). Dacă primul recurge la scrierea unor interogări SQL care să permită afişarea, alterarea ori ştergerea unor informații din bazele de date aferente sitului în cadrul câmpurilor unor formulare sau direct în URI, al doilea constă în „injectarea" în cadrul sistemului, pentru execuție direct în *browser*, a *script*-urilor JavaScript ori VBScript sau a altor tipuri de programe. Aceste atacuri funcționează şi în cazul în care se foloseşte criptarea conexiunilor prin SSL (*Secure Socket Layer*)/TLS (*Transport Layer Security*). Drept exemple de atacuri XSS le menționăm pe acelea în care un sit Web (de exemplu, un forum dedicat consumatorilor unui anumit produs) permite vizitatorilor să trimită marcatori `<img>` (pe care i-am putea considera siguri la prima vedere) via un formular pentru a insera o imagine în cadrul mesajului redactat. Un utilizator răuintenționat ar putea introduce o construcție de genul `<img src="javascript:cod" />` pentru a executa cod JavaScript (acest cod, de pildă, ar putea redirecționa unii vizitatori către alt sit – al concurenței – ori le-ar putea şterge documentele locale grație facilităților oferite de Internet Explorer de acces la sistemul de fişiere al clientului – detalii în (Buraga, 2001) –, cu implicații nefericite asupra reputației sitului).

• inocularea de programe pe calculatorul utilizatorului – prin intermediul *script*-urilor,

plug-in-urilor ori al componentelor ActiveX, atacatorul poate plasa programe de tip *malware* (viruşi, spioni, cai troieni etc.) pe calculatorul clientului, exploatând vulnerabilităţile ori *bug*-urile navigatorului Web. În acest mod, se pot apela programe în mod neautorizat, colecta şi/sau distruge resurse, lansa atacuri spre alte sisteme de calcul, crea uşi ascunse (*traps* sau *backdoors*) permiţând acces ulterior la calculator ori obţinerea unor privilegii etc.

Un posibil atacator poate exploata, de asemenea, configuraţiile incorecte sau implicite ale serverelor sau aplicaţiilor Web. Pentru aceasta nu trebuie decât să recurgă la un motor de căutare pentru a detecta posibile vulnerabilităţi. De exemplu, pentru a avea acces la lista fişierelor dintr-un director, vom putea utiliza Google pentru a formula interogarea `intitle:index.of "parent directory"`. La fel, putem detecta versiunile unor servere Web prezentând *bug*-uri cunoscute care, cu puţin noroc, nu au fost încă remediate – detalii în (Buraga, 2005) şi (Long, 2005).

3.4 Riscuri asupra siturilor Web

Perspectivele economice ale riscurilor de securitate în contextul siturilor Web sunt rezumate în tabelul 1.

Riscuri ameninţând o anumită afacere	Exemple
Pierdere financiară cauzată de o fraudă	Transferul neautorizat de fonduri realizat de un atacator intern sau extern
Furtul de informaţii importante	Obţinerea de acces neautorizat la informaţii confidenţiale privitoare la o tehnologie proprietară ori la date strategice referitoare la planul de marketing
Pierderea unei oportunităţi de afacere datorată nefuncţionării unui serviciu	Oprirea pe o perioadă de timp prea lungă a serviciilor *on-line* oferite, cauzată de atacuri deliberate ori de accidente
Utilizarea neautorizată a resurselor	Exploatarea unor servicii pe care le-a dobândit atacatorul prin intermediul unui acces nelegitim la sistem
Costuri determinate de nesiguranţă	Apariţia unor costuri suplimentare datorate procedurilor şi timpului necesar reabilitării unui sit atacat
Pierderea încrederii sau respectului publicului (clientelei)	Problemele (reale sau doar presupuse) de securitate a sitului conduc la erodarea imaginii companiei

Tabelul 1. *Perspectivele economice ale riscurilor de securitate a siturilor Web*

3.5 Instituirea măsurilor de securitate

Apare întrebarea „La ce nivel trebuie luate măsuri de securitate?”. Răspunsul este că măsurile de siguranţă trebuie luate la oricare nivel, principalele acţiuni fiind inhibarea ascultării mediilor de transmisie, interzicerea accesului fizic la server, instalarea zidurilor de protecţie (*firewall*-urilor), criptarea conexiunilor, monitorizarea şi actualizarea software-ului (sistem de operare, server Web, server de aplicaţii, server de baze de date, biblioteci şi programe aferente etc.), jurnalizarea accesului, educarea utilizatorilor şi adoptarea unor politici generale de securitate (Acostăchioaie, 2003; Oprea, 2003).

Elaborarea politicilor de securitate vizează (Garfinkel & Spafford, 2001; Howard & LeBlanc, 2003; Tanenbaum, 2003):

- planificarea cerinţelor de securitate (se iau în consideraţie asigurarea confidenţialităţii, integrităţii şi disponibilităţii datelor, controlului asupra accesului etc.);
- evidenţierea riscurilor (se vor realiza scenarii de risc şi se vor studia soluţiile care pot fi aplicate în fiecare caz în parte; se va răspunde la întrebări de genul „Cine decide care date sunt considerate importante?”, „Cât de critice sunt datele identificate?”, „Datele vor fi consistente după restaurarea în urma unui incident?”, „Ce pierderi de date vor exista şi cum vor putea fi ele recuperate după un atac soldat cu succes?”, „Există un plan eficient de recuperare de după dezastru?”, „Care va fi perioada în care situl nu va fi operaţional?” şi altele);
- analiza raportului cost-beneficii (trebuie evaluate costurile prevenirii incidentelor de securitate, ale refacerii după dezastru etc.);
- stabilirea politicilor de securitate (se adoptă atât o politică generală, la nivel naţional ori organizaţional, dar şi politici separate pentru diverse domenii protejate; tot aici, se poate recurge la studierea şi aplicarea unor standarde şi reglementări ori recomandări).

Măsurile luate pot fi tehnice, dar şi nontehnice. Trebuie reţinute următoarele principii (Howard & LeBlanc, 2003):

1. atacatorul poate alege cel mai slab punct al sistemului, responsabilitatea noastră fiind cea de a apăra toate aspectele sistemului;

2. ne putem apăra doar împotriva atacurilor cunoscute, dar atacatorul poate exploata vulnerabilități misterioase;
3. persoanele rău-voitoare pot ataca oricând, vigilența trebuind permanent păstrată;
4. atacatorul nu ține cont de legi, reguli, recomandări ori de bunul simț.

Un exemplu de set de măsuri este detaliat în (Buraga, 2005).

3.6 Supraviețuirea şi analiza riscurilor

Un alt aspect important este cel referitor la *supraviețuire* care reprezintă capacitatea unui sistem de a-şi îndeplini misiunea, în timp util, în pofida atacurilor, defectelor sau accidentelor survenite (Acostăchioaie, 2003). Dacă un atac este un eveniment potențial distrugător provocat intenționat de persoane rău-voitoare, un defect este tot un eveniment potențial distrugător cauzat însă de anumite deficiențe ale sistemului sau ale unui factor de care depinde acel sistem (*e.g.*: defecte hardware, *bug*-uri software, erori ale utilizatorilor). Un accident reprezintă un eveniment neprevăzut – de exemplu, un dezastru natural sau o cădere de tensiune.

În mod ideal, sistemul ar trebui să-şi ducă până la capăt misiunea chiar dacă unele componente sau părți ale acestuia sunt afectate ori scoase din uz. Sistemul trebuie măcar să sprijine îndeplinirea funcțiilor vitale (*mission-critical*), unul dintre aspectele de care trebuie să se țină seamă fiind identificarea serviciilor esențiale. De exemplu, în cazul unui sit de comerț electronic, vizitatorul ar trebui să aibă acces la catalogul produselor, chiar dacă modulul de realizare a comenzilor nu este operațional în acel moment. Situl trebuie să fie rezistent la atacuri, pentru aceasta adoptându-se diverse strategii de respingere a atacurilor (validarea obligatorie a datelor provenite de la utilizatori, autentificarea utilizatorilor, utilizarea de *firewall*-uri, protejarea datelor importante prin criptare, acordarea privilegiilor minime etc.). O bună politică de securitate va lua în considerație şi recunoaşterea atacurilor şi a efectelor acestora, aplicându-se tehnici pentru restaurarea informațiilor, limitarea efectelor negative, menținerea/restaurarea serviciilor compromise şi altele. De asemenea, trebuie să ne adaptăm la atacuri, recurgând la strategii pentru îmbunătățirea şanselor de supraviețuire, învățând şi din greşelile făcute.

Evaluarea gradului de siguranță poate fi realizată atât în cadrul organizației, cât şi prin implicarea unei companii externe specializate. Există mai multe metodologii de analiză a riscurilor, dintre care pot fi menționată *DREAD* (*Damage potential, Reproductibility, Exploitability, Affected users, Discoverability*), descrisă în (Howard & LeBlanc, 2003). Ea calculează potențialul distrugerilor pe care le-ar putea cauza un atacator, gradul de apariție şi de succes al unui potențial atac, efortul (timp, expertiză, resurse alocate etc.) care trebuie depus pentru a realiza atacul, numărul de utilizatori afectați şi probabilitatea descoperirii unei vulnerabilități de către atacator).

O metodologie standardizată de testare a securității este *OSSTMM* (*Open Source Security Testing Methodology Manual*) – *www.osstmm.org* – fiind total independentă de factori comerciali, industriali ori politici. Prin prisma OSSTMM, securitatea trebuie să fie prezentă la nivelul telecomunicațiilor, comunicațiilor fără fir, resurselor rețelelor, personalului şi, nu în ultimul rând, la cel fizic.

3.7 Securitatea aplicațiilor Web

Securitatea unei aplicații Web trebuie să ia în considerație arhitectura, logica, codul-sursă şi conținutul în ansamblu. Securitatea aplicației Web nu vizează în principal vulnerabilitățile sistemului de operare ori *bug*-urile unor programe auxiliare, ci se concentrează asupra prevenirii, descoperirii şi remedierii vulnerabilităților codului propriu (realizat de noi). De cele mai multe, vulnerabilitățile unui sit nu sunt „celebre" precum cele ale unor produse bine-cunoscute, cu toate că ar putea fi vulnerabil la o categorie aparte (precum injectarea de cod SQL). Aceasta are drept consecință faptul că nu vom recepționa buletine de informare privitoare la vulnerabili-tățile găsite şi că nu ne putem baza pe repararea codului de către producătorul software-ului, din moment ce este scris de către noi înşine (excepție fac aplicațiile externe integrate în cadrul sitului nostru, precum *phpBB* ori *DotNetNuke*). Vulnerabilitățile detectate vor fi prezente pe

orice platformă (combinație de sistem de sistem de operare, server Web, server de aplicații) şi vor fi independente deseori de securitatea sistemului pe care este exploatat situl. Aceste vulnerabilități pot fi uşor exploatate de persoane rău-voitoare, deoarece *firewall*-urile nu filtrează mesajele HTTP, monitorizarea accesărilor este dificilă şi rareori realizată efectiv, atacatorii nu trebuie să folosească instrumente software sofisticate pentru a-şi atinge scopurile, iar punctele slabe ale aplicației Web pot fi uşor detectate. Conform (Buraga, 2005) şi (Garfinfel & Spafford, 2001), principalele tipurile de vulnerabilități sunt problemele de autentificare, managementul sesiunilor, injectarea de *script*-uri ori comenzi SQL şi expunerea involuntară (sau în urma unui concurs de împrejurări) a informațiilor delicate (*information disclosure*).

Un alt aspect important este cel al asigurării securității serviciilor Web (O'Neill *et al.*, 2003) care necesită integrarea securității aplicațiilor la nivel de întreprindere (*EASI – Enterprise Application Security Integration*), deoarece se poate recurge la tehnologii (soluții) de securitate multiple situate în zone de interes diferite (server Web, componente *middleware*, servere de stocare, aplicații convenționale etc.).

Trebuie remarcat faptul că riscurile de securitate nu vizează numai proprietarul sitului, ci şi utilizatorul final. Din această perspectivă, un sit vulnerabil, nesigur, poate cauza disconforturi financiare (*e.g.*, utilizatorul poate pierde bani ori informații, fiind victima unei fraude *on-line* realizată de un *cracker*), de performanță (datorită blocării navigatorului din pricina unui program ActiveX malițios, acțiunile utilizatorului sunt încetinite ori făcute inefective, cu consecințe grave – de pildă – în cazul unei licitații efectuate pe Web), psihologice (vizitatorii pot experimenta sentimente de insatisfacție în unele situații), sociale (de exemplu, comunicarea *on-line* cu partenerii de muncă ori de afaceri poate avea de suferit în cazul unui atac) ori de timp (navigarea devine tot mai greoaie ori vizitatorul este deturnat, via XSS, de la situl dorit).

4. Concluzii

Din cele descrise mai sus, rezidă faptul că asigurarea securității aplicațiilor destinate Web-ului, mai ales a celor *e-business*, nu este un aspect care trebuie neglijat, ci – dimpotrivă – care prezintă o deosebită importanță.

Articolul a tratat doar aspectele generale ale riscurilor de securitate, fără a detalia unele probleme legate de asigurarea confidențialității, a împiedicării fraudelor de comerț electronic, a realizării plăților electronice. Aceste problematici apelează la tehnologii de criptare sau bazate pe certificate digitale, prezentate în lucrări ca (Acostăchioaie, 2003), (Garfinfel & Spafford, 2001), (O'Neill *et al.*, 2003) şi (Patriciu *et al.*, 2001). Alte considerații privitoare la securitatea aplicațiilor *e-business* sunt reflectate în (Buraga, 2003) şi (Buraga, 2005).

Referințe

(Acostăchioaie, 2003) D. Acostăchioaie, *Securitatea sistemelor Linux*, Polirom, Iaşi, 2003

(Buraga, 2001) S. Buraga, Tehnologii Web, Matrix Rom, Bucureşti, 2001: *http://www.infoiasi.ro/~busaco/books/web.html*

(Buraga, 2003), S. Buraga (coord.), Aplicații Web la cheie, Polirom, Iaşi, 2003: *http://www.infoiasi.ro/~phpapps/*

(Buraga, 2005) S. Buraga, *Proiectarea siturilor Web* (ediția a doua), Polirom, Iaşi, 2005: *http://www.infoiasi.ro/~design/*

(Garfinfel & Spafford, 2001) S. Garfinkel, G. Spafford, *Web Security, Privacy and Commerce*, O'Reilly, 2001

(Howard & LeBlanc, 2003) Howard, M., LeBlanc, D., *Writing Secure Code* (2nd Edition), Microsoft Press, Redmond, 2003

(Long, 2005) J. Long, *Google Hacking for Penetration Testers*, Syngress Publishing, 2005

(Oprea, 2003) D. Oprea, *Protecția şi securitatea informațiilor*, Polirom, Iaşi, 2003

(O'Neill *et al.*, 2003) O'Neill, M. *et al.*, *Web Services Security*, McGraw-Hill/Osborne, 2003

(Patriciu *et al.*, 2001) V. Patriciu *et al.*, *Securitatea comerțului electronic*, Editura All, Bucureşti, 2001

(Tanenbaum, 2003) A. Tanenbaum, *Rețele de calculatoare* (ediția a patra), Byblos, Tg. Mureş, 2003

(W3C, 2005) * * *, *World-Wide Web Consortium*: *www.w3.org*