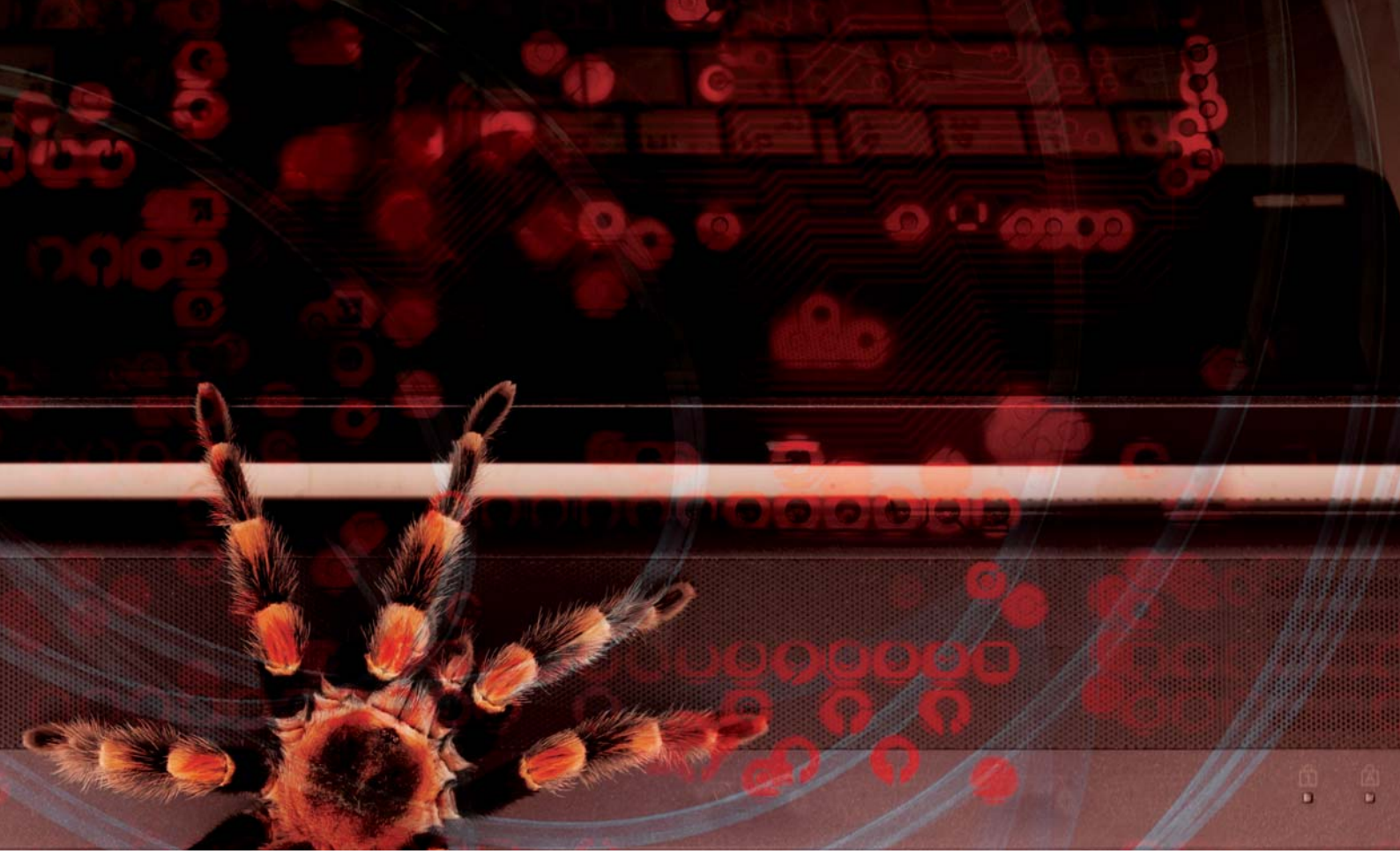

Posúdenie bezpečnosti webovej aplikácie

Prečo je dôležitá bezpečnosť webových aplikácií?

V súčasnej dobe poskytovania on-line elektronických služieb sa webové aplikácie stávajú prirodzených terčom rôznych typov útokov. Motivácia útočníkov je pritom rôznorodá a siaha od (vždy diskutabilnej) snahy ukázať svoje schopnosti pred druhými až po konkrétny úmysel poškodiť dobré meno spoločnosti alebo získať (ukradnúť) citlivé informácie.

Typov útokov na webové aplikácie je mnoho a existuje viacero metodík ich kategorizácie. Jednou z najpoužívanejších je všeobecne akceptovaná kategorizácia podľa OWASP (Open Web Application Security Project), v rámci ktorej sú útoky rozdelené do 10 kategórií. Overenie voči metodike je dôležité tak pre poskytovateľov webových služieb, ako aj pre ich používateľov. Pre poskytovateľov je dôležité otestovať odolnosť webových aplikácií voči známym typom útokov. Pre používateľov je dôležité, že používaná webová aplikácia je spoľahlivá, bezpečná a môžu jej zveriť svoje citlivé údaje.

Ciele posúdenia bezpečnosti webovej aplikácie:

- zvýšiť úroveň bezpečnosti aplikácie odstránením identifikovaných zraniteľností
- zvýšiť odolnosť aplikácie voči známym typom útokov
- zvýšiť spoľahlivosť, bezpečnosť aplikácie a tým aj spokojnosť jej používateľov

Hlavné výhody externého posúdenia bezpečnosti webovej aplikácie:

- nezávislé posúdenie úrovne bezpečnosti webovej aplikácie externým subjektom
- identifikácia zraniteľností v súlade s príslušnou metodikou (HIPAA, PCI, ...)

Tempest
IT makes sense

Testovanie a posúdenie aplikácií

Spoločnosť TEMPEST, a.s. poskytuje testovanie a posúdenie webových aplikácií voči známym typom útokov, ako napr. SQL injection, cross site scripting. Službu realizujú kvalifikovaní a certifikovaní pracovníci pomocou profesionálnych nástrojov a môže prebiehať v štyroch základných módoch.

Typ testu	Aký útok test simuluje	Predpoklady vykonania testu
Testovanie anonymným používateľom z internetového prostredia	Najčastejší typ útoku, ktorý môže vykonať každý, kto má prístup k webovej aplikácii.	Webová aplikácia je dostupná na Internete.
Testovanie autentifikovaným používateľom z internetového prostredia	Útočník je schopný autentifikovať sa do webovej aplikácie, t.j. získal prístupové údaje (napr. meno a heslo).	Webová aplikácia je dostupná na Internete. K dispozícii sú prístupové údaje k aplikácii (napr. meno a heslo).
Testovanie anonymným používateľom z intranetového prostredia	Útok z interného prostredia spoločnosti na webovú aplikáciu.	Útočník sa nachádza v internom prostredí spoločnosti a má dostupnú webovú aplikáciu.
Testovanie autentifikovaným používateľom z intranetového prostredia	Útočník sa nachádza v internom prostredí spoločnosti a je schopný autentifikovať sa do webovej aplikácie, t.j. získal prístupové údaje (napr. meno a heslo).	Útočník sa nachádza v internom prostredí spoločnosti, má dostupnú webovú aplikáciu a pozná prístupové údaje k aplikácii (napr. meno a heslo).

Samotné testovanie a posúdenie webovej aplikácie sa skladá z nasledujúcich činností:

- Príprava testu, t.j. špecifikácia vstupných parametrov, očakávaných výstupov a jednotlivých obmedzení.
- Samotné vykonanie automatizovaného testu webovej aplikácie. Trvanie závisí od zložitosti webovej aplikácie.
- Vyhodnotenie testu a odovzdanie výsledkov v dohodnutom formáte a rozsahu.

Výsledkom testovania a posúdenia sú reporty (dokument), v ktorých sú prehľadne popísané zistenia. Reporty sú štruktúrované podľa požiadaviek príslušných metodík a štandardov. Podporované sú tieto: HIPAA (Health Insurance Portability and Accountability Act), OWASP Top 10 (2004, 2007, 2010), PCI (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley Act of 2002), WASC (Web Application Security Consortium).

Ďalšie služby

Okrem testovania webových aplikácií automatizovaným nástrojom poskytuje v tejto oblasti spoločnosť TEMPEST, a.s. nasledujúce služby:

- White Box testovanie, t.j. analýza kódu s dôrazom na bezpečnostné funkcie.
- Vypracovanie metodiky a zodpovedajúcej dokumentácie pre tvorbu bezpečných webových aplikácií (napr. coding guidelines).

V prípade týchto služieb odhad náročnosti ich realizácie závisí od testovanej webovej aplikácie, a to najmä od jej typu (napr. PHP, ASP, J2EE), rozsahu (napr. počet formulárov, integrácia na iné systémy) a od používaných postupov v spoločnosti počas celého vývojového cyklu webovej aplikácie.

Tempest
IT makes sense