

Penetrační testy

Specializovaný software nebo hackeři odhalují slabá místa

Každé webové řešení je hned od spuštění cílem útoků. Riziko závažných důsledků s časem roste. Penetrační testy, ať pravidelné nebo ad hoc, jsou jednou z cest, jak **riziko narušení vašeho webu či e-shopu minimalizovat**.



Čím je webové řešení složitější, tím více skýtá příležitostí k napadení:

- **pokusy o zahlcení ("shození") vašeho serveru**
- **pokusy o změnu obsahu**
- **průnik k vašim interním nebo zákaznickým datům**
- **nasazení škodlivého kódu, např. s cílem těžby kryptoměn apod.**

Ověříme zranitelnost vašeho webového řešení.



Softwarem určeným k odhalování rizik ve zdrojovém kódu nebo ve spolupráci s odborníky na internetovou bezpečnost budeme simulovat útoky na Váš e-shop či web, abychom ověřili jeho odolnost.



Automatizované penetrační testy

Základním nástrojem testování bezpečnostních rizik by měla být 4x ročně prověrka odolnosti (Deep Scan) specializovaným softwarem - dáme Vám na výběr ze světových lídrů mezi penetračními testy. K odhaleným zranitelnostem ihned připojí naši IT specialisté návrhy možných řešení.



Manuální penetrační testy

Jednou ročně je vhodné doplnit automatické skeny simulovaným útokem na Váš server tzv. etickými hackery. Pokusí se ho vyřadit z provozu, proniknout ke chráněnému obsahu, změnit ho nebo zcizit. Výsledkem je i zde protokol s konkrétními návrhy na odstranění zjištěných zranitelností.



Bug bounty programy

Po provedení předchozích penetračních testů můžete vyhlásit akci pro desítky či stovky etických hackerů - nabídnout odměnu těm, kteří odhalí kritické nedostatky vašeho systému. Čím víc se jich do akce zapojí, tím důkladněji Váš e-shop či web prověří, a tím větší jistotu zabezpečení získáte, pokud žádné bugy nenajdou.

Chraňte svůj server penetračními testy!

Kontaktujte: obchod@fg.cz

www.fg.cz