Základní minimum zabezpečení webových stránek

Vzhledem k tomu, že počet útoků na webové aplikace neubývá, je nezbytné, aby měl každý správce alespoň minimální vědomosti o základních bezpečnostních opatřeních, která mu umožní lépe spát.

ZUZANA DURAČINSKÁ

Mnoho bezpečnostních pravidel provozovatelé webů znají, avšak jejich implementace z různých důvodu absentuje. Jednou z příčin může být fakt, že na rozdíl od funkčních a designových upgradů nejsou bezpečnostní vylepšení a doplňky vidět (pokud se stránky nedostanou pod útok), a proto se jim mnohdy nevěnuje dostatečná podpora.

Přinášíme na základě zkušeností z provozováním služby Skener webu základní bezpečnostní pravidla, která by měl mít každý správce na mysli, když programuje nebo vylepšuje webovou aplikaci. Důležitost a priorita, které udělíte jednotlivým bodům, záleží na službách a zaměření samotné aplikace.

[Šifrované spojení by dnes mělo být standardem na všech webech, kde dochází k výměně informací, které by mohly být při zachycení zneužité.]

1 Pravidelné updaty a sledování zranitelností

Bez ohledu na to, jaké CMS (Content Management System), webový server či doplňky využíváte, je vhodné, ba přímo žádoucí mít všechny jejich verze pravidelně updatované. Zranitelnosti vztahující se k jednotlivým verzím softwaru nejsou žádným internetovým tajemstvím a právě nedůslednost při updatech se často využívá při plošných útocích.

Je také dobré průběžně sledovat e-mailové konference jednotlivých programových doplňků, které při provozu aplikace využíváte. Každá aplikace se označuje mírou rizika, která může být při rozhodování o případném updatu směrodatná.

CVSS (Common Vulnerability Scoring System) je všeobecně uznávanou metodou na hodnocení závažnosti zranitelností. Zranitelnosti s nízkým rizikem označuje podle speciální metodiky vypočítávání skóre v rozmezí od 0–3,9, zranitelnosti se středním rizikem se pohybují v rozmezí od 4,0–6,9 a konečně od 7,0–10 se označují chyby, které mohou představovat vysoké riziko pro samotnou aplikaci.

Aby byl systém vyhledávání (a práce s ním) přehledný a pokud možno neobsahoval zbytečné duplicity, podléhají také zranitelnosti systému označení CVE (Common Vulnerabilities and Exposures). Každé zranitelnosti se udělí unikátní CVE ID s jejím stručným popisem. A ještě malá rada na závěr prvního bodu: pokud nějaké doplňky na webu již nevyužíváte, nenechte je tam zbytečně viset a raději je odinstalujte.

2 Koho zajímá verze vašeho webového serveru

No přece útočníky! Na čem váš web běží a jaké softwarové doplňky na něm využíváte – to není informace, kterou byste chtěli sdílet. Důvod je z části načrtnutý v prvním bodě. Pokud není váš web natolik zajímavý, aby se stal terčem skutečně sofistikovaného útoku, útočník pravděpodobně využije jednu z mnoha známých zranitelností a exploitů.

Míst, kde je možné zveřejnit takové informace, je hned několik, např. ve fingerprintech serveru, hlavičkách, chybových hláškách či ve zdrojovém kódu. Uživatel údaje tohoto typu nepotřebuje a útočníkovi je dát nechcete. Při návrhu aplikace je proto vhodné všechny výstupy, které by mohly tuto informaci obsahovat, ošetřit.

3 Šifrované spojení a certifikáty

Šifrované spojení by dnes mělo být standardem na všech webech, kde nastává výměna informací, které by mohly být při odchycení zneužité (man-in-the-middle attack). Jde například o přihlašování do administrátorského rozhraní, nakupování v e-shopech, přihlašování do aplikace a podobně.

Sice se může zdát, že implementace certifikátu je snadnou záležitostí, ale ze zkušeností se ví, že problémů může nastat hned několik – neplatné certifikáty, certifikát vydaný neuznávanou certifikační autoritou, certifikát vydaný pro jinou doménu nebo certifikáty vydané samotným provozovatelem webu.

Schvalování nedůvěryhodných certifikátů v prohlížečích se tak stává běžnou praxí a jejich používání na