vašich webech není zrovna nejlepším řešením. Abyste měli jistotu, že uživatel bude na stránky přistupovat pouze přes HTTPS, doporučujeme využívat bezpečnostní mechanismus HSTS (HTTP Strict Transport Security).

Ten je zahrnutý v hlavičkách požadavků zabezpečení a říká, že prohlížeč bude zasílat všechnu komunikaci jenom přes HTTPS, a tím ochrání uživatele před útoky typu man-in-the-middle, mezi které patří taky SSL-striping.

4 Veřejně dostupné rozhraní a informace

Uživatelé a administrátoři potřebují pro své přístupy různá rozhraní. Přihlašování do administrace webu či k interním dokumentům by mělo být dostupné pouze z vlastního adresního rozsahu nebo přes VPN (Virtual Private Network).

Přihlašování do administrace webu v kombinaci s neošetřenými vstupy (obrana proti SQL injection), absencí ochrany proti brute forcu či neexistující dostatečnou politikou hesel představují pro aplikaci nepříjemné riziko.

5 Ošetření vstupů

To, že prohlížeče dnes již řadu filtrů jako obranu před různými útoky obsahují, neznamená, že ošetření na straně vstupů můžeme ignorovat. Ať už jde o přihlašování do aplikace, vyhledávání v rámci aplikace nebo různé druhy formulářů, každý vstup by měl mít ošetřené, jaké znaky bude ze strany aplikace přijímat.

Správným „escapováním“ znaků předejdete pokusům o zasílání útočníkových dotazů do SQL databáze či útokům typu XSS (Cross Site Scripting). Jednoduše řečeno, jak často potřebujete přijímat ze strany uživatele znaky typu <, >, „, &?

Jako obranu proti XSS můžete taky využít příznak X-XSS-Protection, který se umísťuje do hlaviček požadavků. Tento příznak vynucuje použití XSS filtru, jenž je v prohlížečích často defaultně nastavený, ale uživatel ho může kdykoliv vypnout.

6 Využívání autorizačních tokenů

CSFR (Cross Site Request Forgery) umožňuje napadnutí stránek zfalšováním požadavku webové aplikace tak, že server nerozliší, zda přišel požadavek od legitimní osoby nebo od útočníka. Obranou může být například sledování refereru HTTP hlavičky nebo sledování HTTP Origin. Oboje však může být pro většinu uživatelů omezující.

Nejefektivnějším způsobem obrany je proto použití autorizačního tokenu. Hodnota tokenu, která je zahrnutá v požadavcích, se porovnává s předtím uloženou hodnotou, požadavek se zpracuje pouze v případě shody jejich hodnot.

Token by měl mít hodnotu, kterou nelze predikovat, a měl by se měnit v závislosti od uživatele a formuláře. Měl by se také měnit při každém novém načtení formuláře uživatelem.

Kvůli možnému oklamání uživatele například překrytím stránky a přepsáním autorizačního tokenu pod záminkou například Captcha je dobré doplnit do hlaviček ještě položku X-Frame-Options. Toto rozšíření hlaviček pak na základě zvolené hodnoty omezí vložení stránek do framu.

[Ve všech uživatelských a administrátorských účtech by měla být implementovaná dostatečně silná politika hesel.]

[Pokud služby na otevřených portech nevyužíváte nebo nemáte dostatečný důvod, proč by daný port měl být otevřený, je lepší jej uzavřít.]

7 Nastavení politiky hesel

Ve všech uživatelských a administrátorských účtech by měla být implementovaná dostatečně silná politika hesel. Požadavky na minimálně osmiznakové heslo, obsahující malá a velká písmena, čísla a speciální znaky, mohou mít v závislosti na hodnotě dat obsažených v aplikaci u uživatelských účtů alespoň doporučující povahu.

V administrátorských účtech by se měly vynucovat. Hesla by se také neměla ukládat v textové podobě a neměla by se zasílat přes internet v otevřené podobě (například do e-mailu po jejich zapomenutí).

8 Implementace DNSSEC

S webovou stránkou přímo souvisí také zabezpečení DNS (Domain Name System) záznamů. DNSSEC zajistí úplnost a integritu informací poskytovaných z DNS. Při jeho zavedení je nutné spolupracovat s registrátorem, který musí část údajů potřebných k využívání DNSSEC uložit do DNS záznamů vaší domény a pak do registru domén.

Pro implementaci této technologie je tedy nezbytné, aby příslušný registrátor správu DNSSEC údajů podporoval. Při registraci domény si to proto raději zkontrolujte.

9 Bezpečně a správně implementované cookies

Cookies obsahují informace o uživatelském sezení, a stávají se tak citlivým prvkem každé webové aplikace. Způsobů jejich implementace je několik.

Hodnota cookie by se měla měnit v závislosti na uživateli, sezení a vykonávaných akcích. Také je třeba myslet na ukončení její platnosti v případě zavření prohlížeče či odhlášení uživatele.

S tím taky souvisí akceptace jen těch cookies, které se zasílají ze serveru (tak aby nebylo možné použít cookies zaslané klientem).

Nezapomeňte také na bezpečnostní flagy „HttpOnly“ a „secure“. Zatímco flag „secure“ zajistí, aby se cookies zasílaly jenom přes šifrované spojení, čímž zabrání jejich odchycení v clear textu, flag „HttpOnly“ zabezpečí, že přístup ke cookies bude možný pouze přes požadavek typu HTTP nebo HTTPS, a zabrání tak přístupu ke cookies například prostřednictvím javascriptu.

10 Last but not least

Nezapomínejte na riziko spojené s otevřenými porty. Pokud služby na otevřených portech nevyužíváte nebo nemáte dostatečný důvod, proč by daný port měl být otevřený, je lepší jej uzavřít.

Nechtěné problémy může způsobit taky příliš velký počet externích přepojení na stránku, například formou reklamy nebo různých odkazů. Přes přímý odkaz na web se taky může šířit nákaza. Zvažte, zda jsou všechny externí odkazy na vašem webu nutné.

Upload souboru přes různé formuláře je dalším prvkem v aplikaci, na který by administrátor neměl zapomínat. Ošetřená by měla být jak velikost, tak druh souboru, který je možné nahrát. ■

Autorka pracuje jako bezpečnostní analytik sdružení CZ.NIC, které provozuje národní bezpečnostní tým CSIRT.CZ