Kontrolný zoznam pre bezpečnosť webových aplikácií

Podobne ako všetky nové technológie, aj webové aplikácie so sebou priniesli nové zraniteľnosti a možnosti kompromitácie organizácie. Existuje celá škála útokov, ktoré môže útočník využiť na získanie prístupu k citlivým informáciám alebo prístupu do systémov, na ktorých sú webové aplikácie prevádzkované. Okrem implementácie opatrení na zaistenie bezpečnosti webových aplikácií je potrebné myslieť aj na zabezpečenie a hardening ich podporných systémov. Nasledovný kontrolný zoznam stručne sumarizuje najdôležitejšie bezpečnostné aspekty pri vývoji a prevádzke webových stránok a je možné ho využiť pri vykonávaní interného auditu bezpečnosti webových aplikácií a webových stránok.

Číslo	Opatrenie	Splnené	Poznámka
BN	**Bezpečný návrh**		
BN1	Webová stránka by mala pozostávať z verejných a privátnych zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.	☐	
BN2	Citlivé informácie musia byť uchovávané v zašifrovanej podobe.	☐	
BN3	Validácia vstupov musí byť vykonávaná ako na strane klienta, tak aj na strane servera.	☐	
BN4	Produkčný a databázový server by mal byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby.	☐	
BN5	Kód by mal byť udržiavaný, prehľadný a dokumentovaný.	☐	
BN6	Prezentačná vrstva musí byť oddelená od logickej vrstvy.	☐	
CR	**Šifrovanie**	**Splnené**	**Poznámka**
CR1	Na webový portál sa musí pristupovať prostredníctvom protokolu HTTPS.	☐	
CR2	Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný webový portál.	☐	
CR3	Webový portál nesmie používať nedôveryhodné alebo exspirované SSL/TLS certifikáty.	☐	
CR4	Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.	☐	
CR5	Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.	☐	
CR6	Webový portál nesmie ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.	☐	
CR7	Webový portál nesmie vkladať nešifrované zdroje bez SSL/TLS do stránok s SSL/TLS.	☐	
PK	**Šifrovacie kľúče a protokoly**	**Splnené**	**Poznámka**

PK1	Webový server nesmie podporovať protokoly SSLv2, SSLv3, TLS 1.0 a TLS 1.1.	□	
PK2	Webový server musí podporovať TLS 1.2	□	
PK3	Webový server by mal podporovať TLS 1.3.	□	
PK4	Webový server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64 bitov.	□	
PK5	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku FREAK.	□	
PK6	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES).	□	
PK7	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku BREACH (Pri SSL/TLS musí byť vypnutá http kompresia).	□	
PK8	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku POODLE.	□	
PK9	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku LOGJAM.	□	
PK10	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku CRIME (vypnúť SSL/TLS kompresiu)	□	
PK11	DÍžka kľúča asymetrickej šifry RSA, DSA v certifikáte by mala byť 4096 bitov.	□	
PK12	Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).	□	
PK13	Webový server by nemal podporovať RC4, DES a 3DES.	□	
PK14	Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi. Pri použití CBC šifier je potrebné použiť ďalšiu autentifikáciu, napríklad HMAC (hashovaný autentifikačný kód správ).	□	
PK15	Webový server nesmie používať exportné šifry.	□	
PK16	Webový server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.	□	
PK17	Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.	□	
PK18	*Konfiguráciu je možné otestovať v SSL teste od Qualys : https://www.ssllabs.com/ssltest/index.html*.	□	
C	**Konfigurácia servera**	**Splnené**	**Poznámka**
C1	Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov.	□	
HH	**HTTP hlavičky a cookies**	**Splnené**	**Poznámka**
HH1	Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security.	□	
HH2	V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.)	□	

HH3	V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.	□	
	Server musí používať hlavičku:		
HH4	X-Frame-Options : SAMEORIGIN // ochrana pred clickjackingom,	□	
HH5	X-XSS-Protection : 1 // čiastočná ochrana pred XSS.	□	
	Konfigurácia webového servera		
S	**Systém**	**Splnené**	**Poznámka**
S1	Systém, nainštalované aplikácie a frameworky musia byť aktuálne z pohľadu bezpečnostných aktualizácií.	□	
S2	Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.	□	

S3	Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.	□	
S4	Na serveri musia byť zatvorené všetky nepoužívané porty.	□	
WS	**Webový server**	**Splnené**	**Poznámka**
WS1	Webový server by mal podporovať iba HTTP metódy POST a GET.	□	
WS2	Webový server nesmie podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.	□	
WS3	Webový server musí byť odolný voči SlowHTTP DoS (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty.)	□	
WS4	Na webovom serveri musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy.	□	
WS5	Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.	□	
WS6	Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.	□	
WS7	Webový server nesmie podporovať funkcionalitu listovania adresára (directory listing, Microsoft IIS tilde directory enumeration).	□	
WS8	Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).	□	
WS9	Z webového servera musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.	□	
	Na webovom serveri by mal byť implementovaný WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:		
WS10	Detekcia a prevencia známych útokov (code injection – SQL, XSS, Command, XPATH),	□	

WS11	Encoding a kontrola používateľských vstupov prostredníctvom whitelistingu.	□	
AD	**Administrácia**	**Splnené**	**Poznámka**
AD1	Administračné rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).	□	
AD2	Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.	□	
AD3	Všetky servery a syslog servery musia byť synchronizované s NTP serverom.	□	
AD4	Administračné rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.	□	
AP	**Aplikácia (webový portál)**	**Splnené**	**Poznámka**
AP1	Aplikácia musí ošetrovať všetky chyby a výnimky.	□	
AP2	Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.	□	
AP3	V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.	□	
AP4	Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).	□	
AP5	Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.	□	
AP6	Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.	□	
AP7	Aplikácia nesmie ukladať citlivé údaje (napríklad session token) v URL adrese.	□	
AP8	Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy na SR).	□	
AP9	Aplikácie nesmie používať odkazy na nedôveryhodné externé zdroje.	□	
AP10	Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).	□	
AP11	Aplikácia nesmie používať funkciu eval().	□	
AP12	Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.	□	
AA	**Autentizácia a autorizácia**	**Splnené**	**Poznámka**
AA1	Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).	□	

AA2	Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu.	□	
AA3	Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.	□	
AA4	Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.	□	
AA5	Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.	□	
AA6	Aplikácia musí vyžadovať používanie silných hesiel (dĺžka aspoň 14 znakov, aspoň jedno veľké písmeno, malé písmeno, číslo a špeciálny znak).	□	
AA7	Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.	□	
AA8	Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.	□	
AA9	Aplikácia musí po zmene hesla vyžadovať reautentizáciu.	□	
AA10	Aplikácia by mala pri zmene hesla notifikovať používateľa zaslaním verifikačného emailu.	□	
AA11	Aplikácia musí uložené heslá hashovať prostredníctvom odporúčaných kryptografických hashovacích funkcií a musí používať salt.	□	
AA12	Pri ukladaná hesiel by mal byť použitý hashovací algoritmus minimálne SHA-256. Nesmie sa používať algoritmus MD5.	□	
AA13	Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti.	□	
AA14	Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.	□	
AA15	Aplikácia musí podporovať simultánne paralelné prihlásenie iba z jednej verejnej IP adresy.	□	
AA16	Aplikácia musí pri zmene verejnej IP adresy požadovať reautentifikáciu.	□	
AA17	Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lock-out) po istom počte neúspešných pokusov (5) o prihlásenie.	□	
AA18	Zamknutie účtu po 5 neúspešných pokusoch o prihlásenie musí trvať aspoň 10 minút.	□	
AA19	Zamknutie účtu po 5 neúspešných pokusoch o prihlásenie do kritického systému by malo trvať aspoň hodinu.	□	
AA20	Je potrebné vytvárať log záznamy všetkých pokusov o autentizáciu (log-in, log-out, neúspešný log-in, žiadosť o zmenu hesla).	□	
AA21	V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.	□	
AA22	Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať.	□	
AA23	Aplikácia nesmie pre kritické systémy umožniť funkcionalitu zapamätania si hesla.	□	

UI	Používateľské vstupy	Splnené	Poznámka
UI1	Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.	□	
UI2	Aplikácia by mala používať parametrizované SQL požiadavky (queries).	□	
UI3	Aplikácia nesmie využívať používateľské vstupy bez kontroly na tvorenie SQL dopytov.	□	
UI4	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SQL príkazoch (statements).	□	
	Napríklad :		
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dotaze alebo parametri príkazu operačného systému.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte REST API.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query).	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI príkazoch (statements).	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách.	□	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych výrazoch.	□	
SS	**Relácie**	**Splnené**	**Poznámka**
SS1	Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.	□	
SS2	Aplikácia nesmie povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.	□	
SS3	Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.	□	
SS4	Na generovanie CSRF tokenov musí aplikácia kryptograficky silný generátor pseudonáhodných čísel.	□	
SS5	Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie.	□	

SS6	Pri zmene prihlasovacích údajov (credentials) musí aplikácia znovu vygenerovať identifikátor relácie.	□	
SS7	Pri zmene prihlasovacích údajov (credentials) musí aplikácia zneplatniť ostatné relácie.	□	
SS8	Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.	□	
SS9	Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.	□	
SS10	Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.	□	
SS11	Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).	□	
SS12	Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.	□	
SS13	Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.	□	
SS14	Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.	□	
SS15	Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia.	□	
SS16	Relácia musí byť zviazaná s klientskou IP adresou.	□	
SS17	Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.	□	
FU	**Nahrávanie súborov**	**Splnené**	**Poznámka**
FU1	Aplikácia musí nahrávané súbory ukladať mimo koreňového súboru pre dokumenty (document root), kde súčasne nesmie byť možnosť listovania adresára a nesmie byť možnosť interpretovať nahraté súbory ako napríklad skripty (PHP, ASP, JSP).	□	
FU2	Aplikácia by nemala spúšťať a vyhodnocovať (evaluate) nahraté súbory.	□	
FU3	Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.	□	
FU4	Aplikácia musí umožniť nahrávanie iba špecifických typov súborov a kontrolovať nielen ich príponu, ale aj MIME typ.	□	
FU5	Aplikácia musí nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.	□	
CO	**Obsah**	**Splnené**	**Poznámka**
CO1	Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.	□	
CO2	Aplikácia by mala pre všetky poskytované stránky definovať „character set“.	□	
PX	**Spracovanie XML**	**Splnené**	**Poznámka**
PX1	Aplikácia nesmie podporovať XML external entity expansion.	□	
PX2	Aplikácia nesmie podporovať parsovanie XML external DTD.	□	

PX3	Aplikácia nesmie podporovať všetky nadbytočné alebo nebezpečné XML rozšírenia.	□	
PX4	Aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.	□	
MI	**Rôzne**	**Splnené**	**Poznámka**
MI1	Aplikácia nesmie podporovať presmerovaniena používateľom poskytnuté externé umiestnenia.	□	
MI2	Aplikácia musí obmedziť krížový prístup k doménam prostredníctvom whitelistingu.	□	
MI3	Aplikácia musí pre všetky emailové funkcionality implementovať rate limiting.	□	
MI4	Aplikácia musí pre všetky zdrojovo intenzívne funkcionality implementovať rate limiting.	□	
MI5	Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.	□	