



Kontrolný zoznam pre bezpečnosť webových aplikácií

Odporúčanie VJ CSIRT

08.04.2024

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.	<input type="checkbox"/>	
BN2	Citlivé informácie musia byť uchovávané v zašifrovanej podobe.	<input type="checkbox"/>	
BN3	Validácia vstupov musí byť vykonávaná ako na strane klienta, tak aj na strane servera.	<input type="checkbox"/>	
BN4	Produkčný a databázový server by mal byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby.	<input type="checkbox"/>	
BN5	Kód by mal byť udržiavaný, prehľadný a dokumentovaný.	<input type="checkbox"/>	
BN6	Prezentačná vrstva musí byť oddelená od logickej vrstvy.	<input type="checkbox"/>	
CR	Šifrovanie	Splnené	Poznámka
CR1	Na webový portál sa musí pristupovať prostredníctvom protokolu HTTPS.	<input type="checkbox"/>	
CR2	Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný webový portál.	<input type="checkbox"/>	
CR3	Webový portál nesmie používať nedôveryhodné alebo exspirované SSL/TLS certifikáty.	<input type="checkbox"/>	

CR4	Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti, sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.	<input type="checkbox"/>	
CR5	Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.	<input type="checkbox"/>	
CR6	Webový portál nesmie ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.	<input type="checkbox"/>	
CR7	Webový portál nesmie vkladať nešifrované zdroje bez SSL/TLS do stránok s SSL/TLS.	<input type="checkbox"/>	
PK	Šifrovacie kľúče a protokoly	Splnené	Poznámka
PK1	Webový server nesmie podporovať protokoly SSLv1, SSLv2, SSLv3, TLS 1.0 a TLS 1.1.	<input type="checkbox"/>	
PK2	Webový server musí podporovať TLS 1.2.	<input type="checkbox"/>	
PK3	Webový server by mal podporovať TLS 1.3.	<input type="checkbox"/>	
PK4	Webový server by nemal podporovať šifry s kľúčom kratším ako 128 bitov a blokom kratším ako 128 bitov.	<input type="checkbox"/>	
PK5	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku FREAK.	<input type="checkbox"/>	
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).	<input type="checkbox"/>	
PK7	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku BREACH (Pri SSL/TLS musí byť vypnutá HTTP kompresia).	<input type="checkbox"/>	
PK8	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku POODLE.	<input type="checkbox"/>	
PK9	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku LOGJAM.	<input type="checkbox"/>	
PK10	Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku CRIME (vypnúť SSL/TLS kompresiu).	<input type="checkbox"/>	

PK11	Dĺžka kľúča asymetrickej šifry RSA, DSA v certifikáte by mala byť 4096 bitov.	<input type="checkbox"/>	
PK12	Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).	<input type="checkbox"/>	
PK13	Webový server by nemal podporovať RC4, DES a 3DES.	<input type="checkbox"/>	
PK14	Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi. Pri použití CBC šifrier je potrebné použiť ďalšiu autentifikáciu, napríklad HMAC (hashovaný autentifikačný kód správ).	<input type="checkbox"/>	
PK15	Webový server nesmie používať exportné šifry.	<input type="checkbox"/>	
PK16	Webový server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.	<input type="checkbox"/>	
PK17	Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.	<input type="checkbox"/>	
PK18	Konfiguráciu je možné otestovať v SSL teste od Qualys : https://www.ssllabs.com/ssltest/ .	<input type="checkbox"/>	
C	Konfigurácia servera	Splnené	Poznámka
C1	Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov.	<input type="checkbox"/>	
HH	HTTP hlavičky a cookies	Splnené	Poznámka
HH1	Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security.	<input type="checkbox"/>	
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.)	<input type="checkbox"/>	
HH3	V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.	<input type="checkbox"/>	
	Server musí používať hlavičku:		

HH4	Content-Security-Policy: frame-ancestors na hodnotu 'none' alebo 'self', prípadne iné nevyhnutné výnimky. // ochrana pred clickjackingom	<input type="checkbox"/>	
HH5	X-XSS-Protection : 1 // čiastočná ochrana pred XSS	<input type="checkbox"/>	
HH6	Content-Security-Policy: script-src na hodnotu 'self' // čiastočná ochrana pred XSS	<input type="checkbox"/>	
Konfigurácia webového servera			
S	Systém	Splnené	Poznámka
S1	Systém, nainštalované aplikácie a frameworky musia byť aktuálne z pohľadu bezpečnostných aktualizácií.	<input type="checkbox"/>	
S2	Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.	<input type="checkbox"/>	
S3	Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.	<input type="checkbox"/>	
S4	Na serveri musia byť zatvorené všetky nepoužívané porty.	<input type="checkbox"/>	
WS	Webový server	Splnené	Poznámka
WS1	Webový server by mal správne a konzistentne implementovať spracovanie hlavičky Content-Length a Transfer-Encoding.	<input type="checkbox"/>	
WS2	Webový server nesmie podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.	<input type="checkbox"/>	
WS3	Webový server musí byť odolný voči SlowHTTP DoS (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty).	<input type="checkbox"/>	
WS4	Na webovom serveri musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy.	<input type="checkbox"/>	
WS5	Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.	<input type="checkbox"/>	

WS6	Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.	<input type="checkbox"/>	
WS7	Webový server nesmie podporovať funkcionality listovania adresára (directory listing, Microsoft IIS tilde directory enumeration).	<input type="checkbox"/>	
WS8	Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).	<input type="checkbox"/>	
WS9	Z webového servera musia byť odstránené všetky ladiace výstupy, dočasné súbory a nepotrebné zdrojové kódy.	<input type="checkbox"/>	
	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).	<input type="checkbox"/>	
WS11	Encoding a kontrola používateľských vstupov prostredníctvom whitelistingu.	<input type="checkbox"/>	
AD	Administrácia	Splnené	Poznámka
AD1	Administračné rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete / VPN prístupy).	<input type="checkbox"/>	
AD2	Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.	<input type="checkbox"/>	
AD3	Všetky servery a syslog servery musia byť synchronizované s NTP serverom.	<input type="checkbox"/>	
AD4	Administračné rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.	<input type="checkbox"/>	
AP	Aplikácia (webový portál)	Splnené	Poznámka
AP1	Aplikácia musí ošetrovať všetky chyby a výnimky.	<input type="checkbox"/>	
AP2	Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.	<input type="checkbox"/>	

AP3	V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.	<input type="checkbox"/>	
AP4	Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).	<input type="checkbox"/>	
AP5	Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.	<input type="checkbox"/>	
AP6	Pre posielanie citlivých a autentifikačných údajov musí byť vynucované spojenie HTTPS.	<input type="checkbox"/>	
AP7	Aplikácia nesmie ukladať citlivé údaje (napríklad session token) v URL adrese.	<input type="checkbox"/>	
AP8	Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy v SR).	<input type="checkbox"/>	
AP9	Aplikácia nesmie používať odkazy na nedôveryhodné externé zdroje.	<input type="checkbox"/>	
AP10	Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).	<input type="checkbox"/>	
AP11	Aplikácia nesmie používať funkciu eval().	<input type="checkbox"/>	
AP12	Z aplikácie musia byť odstránené všetky ladiace výstupy.	<input type="checkbox"/>	
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).	<input type="checkbox"/>	
AA2	Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu.	<input type="checkbox"/>	
AA3	Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.	<input type="checkbox"/>	
AA4	Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.	<input type="checkbox"/>	

AA5	Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.	<input type="checkbox"/>	
AA6	Aplikácia musí vyžadovať používanie silných hesiel (dĺžka aspoň 14 znakov, aspoň jedno veľké písmeno, malé písmeno, číslo a špeciálny znak).	<input type="checkbox"/>	
AA7	Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.	<input type="checkbox"/>	
AA8	Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.	<input type="checkbox"/>	
AA9	Aplikácia musí po zmene hesla vyžadovať reautentizáciu.	<input type="checkbox"/>	
AA10	Aplikácia by mala pri zmene hesla notifikovať používateľa zaslaním verifikačného emailu.	<input type="checkbox"/>	
AA11	Aplikácia musí uložené heslá hashovať prostredníctvom odporúčaných kryptografických hashovacích funkcií a musí používať soľ.	<input type="checkbox"/>	
AA12	Pri ukladaní hesiel by mal byť použitý hashovací algoritmus minimálne SHA-256. Nesmie sa používať algoritmus MD5.	<input type="checkbox"/>	
AA13	Aplikácia musí implementovať funkcionality pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti.	<input type="checkbox"/>	
AA14	Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.	<input type="checkbox"/>	
AA15	Aplikácia musí podporovať simultánne paralelné prihlásenie iba z jednej verejnej IP adresy.	<input type="checkbox"/>	
AA16	Aplikácia musí pri zmene verejnej IP adresy požadovať reautentifikáciu.	<input type="checkbox"/>	
AA17	Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lock-out) po istom počte neúspešných pokusov (5) o prihlásenie.	<input type="checkbox"/>	
AA18	Zamknutie účtu po 5 neúspešných pokusoch o prihlásenie musí trvať aspoň 10 minút.	<input type="checkbox"/>	

AA19	Zamknutie účtu po 5 neúspešných pokusoch o prihlásenie do kritického systému by malo trvať aspoň hodinu.	<input type="checkbox"/>	
AA20	Je odporúčané vytvárať log záznamy všetkých pokusov o autentizáciu (log-in, log-out, neúspešný log-in, žiadosť o zmenu hesla).	<input type="checkbox"/>	
AA21	V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.	<input type="checkbox"/>	
AA22	Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať.	<input type="checkbox"/>	
AA23	Aplikácia nesmie pre kritické systémy umožniť funkčnosť zapamätania si hesla.	<input type="checkbox"/>	
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.	<input type="checkbox"/>	
UI2	Aplikácia by mala používať parametrizované databázové dopyty (queries).	<input type="checkbox"/>	
UI3	Aplikácia nesmie využívať používateľské vstupy bez kontroly na tvorenie databázových dopytov.	<input type="checkbox"/>	
UI4	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kóde, napríklad:		
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dotaze alebo parametri príkazu operačného systému.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch.	<input type="checkbox"/>	

	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v PDF dokumentoch.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query).	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI príkazoch (statements).	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych výrazoch.	<input type="checkbox"/>	
	Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v renderovaných šablónach.	<input type="checkbox"/>	
SS	Relácie	Splnené	Poznámka
SS1	Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.	<input type="checkbox"/>	
SS2	Aplikácia nesmie povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.	<input type="checkbox"/>	
SS3	Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.	<input type="checkbox"/>	
SS4	Na generovanie CSRF tokenov musí aplikácia používať kryptograficky silný generátor pseudonáhodných čísel.	<input type="checkbox"/>	
SS5	Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie.	<input type="checkbox"/>	

SS6	Pri zmene prihlasovacích údajov (credentials) musí aplikácia znovu vygenerovať identifikátor relácie.	<input type="checkbox"/>	
SS7	Pri zmene prihlasovacích údajov (credentials) musí aplikácia zneplatniť všetky ostatné relácie.	<input type="checkbox"/>	
SS8	Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.	<input type="checkbox"/>	
SS9	Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.	<input type="checkbox"/>	
SS10	Pre relačné (session) cookies musí aplikácia nastaviť SameSite flag na hodnotu 'strict' alebo aspoň 'lax'.	<input type="checkbox"/>	
SS11	Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.	<input type="checkbox"/>	
SS12	Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).	<input type="checkbox"/>	
SS13	Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.	<input type="checkbox"/>	
SS14	Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.	<input type="checkbox"/>	
SS15	Aplikácia musí zamietat' neznáme relačné identifikátory zo strany klienta.	<input type="checkbox"/>	
SS16	Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia.	<input type="checkbox"/>	
SS17	Aplikácia musí vynucovať periodickú expiráciu a zneplatnenie relácií.	<input type="checkbox"/>	
SS18	Relácia by mala byť zviazaná s klientskou IP adresou.	<input type="checkbox"/>	
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).	<input type="checkbox"/>	
FU2	Aplikácia by nemala spúšťať a vyhodnocovať (evaluate) nahraté súbory.	<input type="checkbox"/>	

FU3	Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.	<input type="checkbox"/>	
FU4	Aplikácia musí umožniť nahrávanie iba špecifických typov súborov a kontrolovať nielen ich príponu, ale aj MIME typ, prípadne kontrolovať obsah súboru na úvodné/záverečné bajty.	<input type="checkbox"/>	
FU5	Aplikácia musí nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.	<input type="checkbox"/>	
CO	Obsah	Splnené	Poznámka
CO1	Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.	<input type="checkbox"/>	
CO2	Aplikácia by mala pre všetky poskytované stránky definovať „character set“.	<input type="checkbox"/>	
PX	Spracovanie XML	Splnené	Poznámka
PX1	Aplikácia nesmie podporovať XML external entity expansion.	<input type="checkbox"/>	
PX2	Aplikácia nesmie podporovať parsovanie XML external DTD.	<input type="checkbox"/>	
PX3	Aplikácia nesmie podporovať žiadne nadbytočné alebo nebezpečné XML rozšírenia.	<input type="checkbox"/>	
PX4	Aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.	<input type="checkbox"/>	
MI	Rôzne	Splnené	Poznámka
MI1	Aplikácia nesmie podporovať presmerovanie na používateľom poskytnuté externé umiestnenia.	<input type="checkbox"/>	
MI2	Aplikácia musí pre všetky emailové funkcionality implementovať rate limiting.	<input type="checkbox"/>	
MI3	Aplikácia musí pre všetky zdrojovo náročné funkcionality implementovať rate limiting.	<input type="checkbox"/>	
MI4	Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.	<input type="checkbox"/>	