INNANRÍKISRÁÐUNEYTIÐ

Útfyllt af:	
Dags:	
vefsvæði / lén:	

UT-Vefhandbók

A.1.3.1 Gátlisti við val á veflausn - öryggisþættir

Gátlisti sem hægt er að nota við val á veflausn.
Helstu öryggiskröfur veflausnar eru listaðar upp.

Samantekt yfir atriði tengt vali á veflausn

Atriði	Athugasemdir
Öryggisúttekt	
☐ Hefur verið framkvæmd öryggisúttekt á viðkomandi veflausn samkvæmt kafla 2.5. í vefhandbók?	
☐ Ef slík öryggisúttekt hefur verið framkvæmd, var það gert af óháðum þriðja aðila?	
☐ Hefur verið gerð skýrsla um niðurstöður öryggisúttektar?	
☐ Hafa verið birtar upplýsingar um þekkta veikleika í vefumsjónarkerfi?	
Öryggisuppfærslur	
☐ Hafa verið gefnar út öryggisuppfærslur fyrir vefumsjónarkerfið?	
☐ Er gert ráð fyrir að öryggisuppfærslur verði viðskiptavinum að kostnaðarlausu?	
Tilkynningar	
☐ Hefur verið skilgreint ferli um að viðskiptavinir verði upplýstir um nýjungar í þróun lausnarinnar og þá sérstaklega ef öryggisgallar finnast í veflausninni?	
☐ Hefur verið skilgreint ferli um að tilkynnningar verði reglulega gefnar út með tilliti til öryggisveikleika sem hafa fundist og verið lagaðir?	
☐ Hafa uppfærslur á veflausn verið skjalaðar og upplýsingum um áhrif breytinga komið á framfæri við verkkaupa?	
Dulkóðun og öryggi	
☐ Styður lausnin dulkóðun upplýsinga í gagnagrunni?	
☐ Styður lausnin við þekkta auðkennistaðla s.s. HTTPS/SSL, SFTP o.s.frv.? SSL (Secure Socket Layer) er samskiptastaðall sem tryggir dulkóðuð samskipti. Hægt er að nota SSL til þess að dulkóða ýmis samskipti, meðal annars vefumferð (Hyper Ttext Transfer Protocol), þá er talaða um HTTPS (Hyper Text Transfer Protocol Secured). SFTP stendur fyrir Secured FTP og eru þá dulkóðuð FTP samskipti.	
☐ Býður lausnin upp á dulkóðun viðkvæmra gagna s.s. kortaupplýsinga, lykilorða o.s.frv.?	
Lykilorðastefna	
☐ Hafa kröfur til lykilorða í veflausninni, bæði fyrir aðgang umsjónaraðila og notenda, verið skilgreindar?	
☐ Ef svo er, hafa kröfur verið virkjaðar í samræmi við bestu starfsvenjur? Er Islykilinn notaður þar sem því verður komið við? I öðrum tilfellum þar sem notast verður við notendanöfn og lykilorð er þá hugað að lengd lykilorða, líftíma lykilorða, flækjustigi (samblanda af hástöfum, bókstöfum, táknum) og endurnýjun lykilorða.	
☐ Eru lykilorð dulkóðuð í gagnagrunni veflausnar?	
Annað	
☐ Styður veflausnin fullnægjandi aðgangsstýringar í samræmi við áhættumat? T.d. að gagnagrunni, vefviðmóti, adminkerfum o.fl.?	
☐ Býður lausnin upp á aðskilnað milli þróunar- og raunumhverfis?	
☐ Styður lausnin aðgangsstýringar byggðar á aðgangshópum og hlutverkum?	

Útfyllt af:	
Dags:	
vefsvæði / lén:	

Gátlisti sem hægt er að nota við kaup á þjónustu hjá þriðja aðila. Öryggismál tengt þjónustu þriðja aðila.

A.1.3.2 Gátlisti við val á þjónustuaðilum

Samantekt yfir öryggisatriði tengt vali á þjónustuaðilum

Atriði	Athugasemdir
Stjórnkerfi og vottanir	
☐ Hefur viðkomandi þjónustuaðili fengið ISO/IEC 27001 vottun?	
ISO/IEC 27001 – stjórnkerfi upplýsingaöryggis (http://www.stadlar.is/). ISO/IEC 27001 er alþjóðlegur staðall um innleiðingu og viðhald á stjórnkerfi upplýsingaöryggis.	
☐ Ef svo er, nær umfang vottunarinnar yfir þá þjónustu sem verið er að bjóða upp á?	
☐ Ef svo er ekki, er verið að vinna eftir verklagi samkvæmt ISO/IEC 27001?	
☐ Uppfyllir þjónustuaðili PCIDSS staðalinn?	
PCI- DSS – kröfur um vistun og meðhöndlun kortaupplýsinga (http://greidsluveitan.is/fyrirtaekid/verkefni/pci/). PCI-DSS er staðall sem skilgreinir öryggiskröfur fyrir aðila sem meðhöndla greiðslukortaupplýsingar.	
☐ Starfar þjónustuaðili samkvæmt ITIL (Information Technology Infrastructure Library) stjórnkerfi um þjónustu og rekstur?	
ITIL - Information Technology Infrastructure Library (http://www.itil-officialsite.com/) - ITIL er stuðningsstaðall sem er hugsaður fyrir þjónustustjórnun upplýsingakerfa. Sjá ISO 20000 fyrir nánari upplýsingar. ISO 20000 er alþjóðlegur staðall um þjónustustjórnun upplýsingakerfa.	
☐ Er talið að þjónustuaðili búi yfir nægilegri tæknilegri þekkingu og getu til að þjónusta verkkaupa?	
☐ Liggja skriflegar lýsingar á verkferlum sem eru mikilvægar fyrir rekstur og öryggi upplýsingakerfa þjónustuaðila?	
☐ Hefur verið unnið samkvæmt skjöluðu og formföstu þróunarferli við þróun veflausna?	
☐ Hefur verið unnið samkvæmt viðurkenndum verkefnastjórnunarferlum?	
Öryggisafritunarkröfur	
☐ Hefur verið skilgreint ferli varðandi öryggisafritunarkröfur vegna þeirra gagna sem vistuð eru hjá viðkomandi hýsingaraðila?	
☐ Hefur verið skilgreint ferli varðandi hámarks endurheimtutíma ef til kerfishruns kæmi og það þyrfti að endurheimta kerfið frá öryggisafriti?	
☐ Hefur verið gerð viðlagaáætlun og mun viðkomandi veflausn falla undir þá viðlagaáætlun?	
☐ Hefur verið skilgreint ferli að prófa skuli að endurheimta kerfi frá öryggisafriti að lágmarki einu sinni á ári?	
Öryggisuppfærslur	
☐ Hefur verið skilgreint ferli við uppsetningu öryggisuppfærslna fyrir stýrikerfi og veflausnir þannig að þær verði settar inn um leið og nýjar öryggisuppfærslur eru gefnar út? Eða að lágmarki innan þriggja daga frá því að öryggisuppfærslur eru gefnar út?	
☐ Hafa öryggisuppfærslur verið prófaðar í viðeigandi umhverfi áður en kerfi eru uppfærð?	
Frávikaskráning og vöktun	
☐ Hefur verið viðhöfð frávikaskráning á rekstrarumhverfi?	
☐ Er frávikum komið á framfæri til verkkaupa með reglubundum hætti?	
☐ Eru haldnir stöðufundir með verkkaupa til að koma á framfæri upplýsingum um frávik og vandamál tengd þjónustu?	
Hýsingarumhverfi: (hýsingaraðili)	
☐ Uppfyllir hýsingarumhverfi almennt viðurkenndar kröfur um umhverfisvarnir?	
Helstu umhverfisvarnir eru varaaflgjafi, reykskynjarar, sjálfvirkt slökkvikerfi, hita- og rakaskynjarar, kælikerfi og upphækkað kerfisgólf?	
☐ Hefur aðgangur að hýsingarumhverfi verið takmarkaður við skilgreinda aðila sem þurfa aðgang starfsins vegna?	
☐ Er til staðar neyðaráætlun hjá hýsingaraðila um endurheimt veflausna ef til áfalla kemur?	

Nánari upplýsingar er að finna í handbók um opinbera þjónustusamninga

INNANRÍKISRÁÐUNEYTIÐ

Útfyllt af:	
Dags:	
vefsvæði / lén:	

Gátlisti sem fjallar um afritun á gögnum veflausnar og framkvæmd prófanna á afritunarferlinu.

UT-Vefhandbók

A.1.6.2 Gátlisti sem fjallar um afritun á gögnum

Samantekt yfir atriði tengd afritun gagna

Atriði	Athugasemdir
Öryggisafritun	
☐ Hefur verið skilgreint hvaða gögn eru vistuð í veflausn miðað við tilgang lausnarinnar?	
☐ Hefur verið skilgreint ferli við athugun á hvort kortaupplýsingar, innskráningargögn, persónugreinanlegar upplýsingar o.fl. séu vistuð í veflausn?	
☐ Hefur verið skilgreint hvaða gögn og/eða veflausn á að taka öryggisafrit af?	
☐ Hefur lýsing á afritun gagna verið skjöluð (afritunarstefna)?	
☐ Hefur verið gerð krafa um vistun gagna samkvæmt opinberum kröfum, s.s. lögum um persónuvernd, reglum Þjóðskjalasafns um rafræn opinber gögn og skil á þeim?	
☐ Hefur verið skilgreint hversu oft þarf að taka öryggisafrit af viðkomandi gögnum og/eða veflausn? Í þessu samhengi er oft talað um ásættanlegt gagnatap. Ef öryggisafrit er tekið einu sinni á dag, þá þýðir það að það sé ásættanlegt að tapa gögnum sem bárust og voru vistuð síðustu 24 klukkutímana.	
☐ Hefur geymslutími gagna verið skilgreindur og skjalaður?	
☐ Hefur ábyrðaaðili gagna í veflausn verið skilgreindur?	
☐ Hafa verið gerðar verklagsreglur um hvenær og hvernig eyða skuli gögnum?	
☐ Ef afritun gagna er útvistuð, hefur verið skilgreindur ábyrgðaraðli fyrir eftirlit með framkvæmd afritunar?	
Prófanir öryggisafritunar	
☐ Hefur verið skilgreint hversu oft og hvenær beri að prófa að endurheimta gögn frá öryggisafriti? Þetta er gert til þess að staðfesta annars vegar að verið sé að afrita viðkomandi gögn á endurheimtanlegan hátt og hins vegar að hægt sé að endurheimta veflausnina í heild sinni með nauðsynlegri virkni.	
☐ Hafa verið gerðar prófanir á endurheimt gagna í skjöluðu ferli og endurheimt staðfest af ábyrgðaraðila? Ef brotist er inn á veflausn / vefsíðu, er tryggt að öryggisveikleiki sé ekki til staðar ef endurheimta á af öryggisafriti.	
Vistun öryggisafrita og framkvæmd	
☐ Hafa afrit verið vistuð á öruggum stað í hæfilegri fjarlægð frá frumgögnum?	
☐ Hafa afritunarmiðlar verið merktir á fullnægjandi hátt?	
☐ Hafa frávik í afritun verið skráð niður og þeim fylgt eftir af ábyrgðaraðila?	
☐ Hefur aðgengi að afritum verið takmarkað við samþykkta aðila?	

Útfyllt af:	
Dags:	
vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

Gátlisti varðandi aðgangsstýringar að veflausn og gögnum.

UT-Vefhandbók

A. 1.6.2 Gátlisti varðandi aðgangsstýringar

Samantekt yfir atriði tengt aðgangsstýringum

Atriði	Athugasemdir
Viðkvæmni gagna	
☐ Hefur viðkvæmni gagna sem verið er að vinna með verið kortlögð og þörf á dulkóðun metin?	
☐ Er búið að virkja SSL/TLS? SSL (Secure Socket Layer) er samskiptastaðall yfir/um dulkóðun. Hægt er að nota SSL til þess að dulkóða ýmis samskipti, meðal annars vefumferð (Hyper Text Transfer Protocol), þá er talað um HTTPS (Hyper Text Transfer Protocol Secured). TLS (Transfer Layer Security) er dulkóðunar samskiptastaðall sem hefur tekið við af SSL.	
☐ Ef verið er að nota SSL/TLS, eru rafræn skilríki staðfest af viðurkenndum aðila? Dæmi um viðurkennda aðila: Verisign, Comodo, NetLock, GlobalSign o.fl.	
☐ Eru aðgerðir notenda í veflausninni skráðar (atburðaskráning aðgerða)?	
Aðgangsstjórnun að veflausn og undirliggjandi gagnagrunni	
☐ Hefur aðgangsstýringarferli að veflausn verið skilgreint? Hvernig á að óska eftir aðgangi? Hvernig á að óska eftir því að aðgangi sé lokað? Hverjir þurfa að samþykkja aðgangsbeiðnir?	
☐ Hefur aðgangur þjónustuaðila verið skilgreindur fyrir ákveðið tímabil? Æskilegt er að aðgangur þjónustuaðilans sé eins takmarkaður og mögulegt er.	
☐ Er skilgreindur aðgangur hópa byggður á starfshlutverki og ábyrgð?	
☐ Hafa aðgangsheimildir verið skilgreindar þannig að notendur fá eingöngu aðgang að þeim heimildum sem eru nauðsynlegar (least privilege)?	
☐ Hafa eigendur og ábyrgðaraðilar að veflausn og gögnum lausnarinnar verið skilgreindir?	
☐ Hefur verið ákveðið að notast sé við einkvæm (persónuleg/persónubundin) notendanöfn?	
☐ Hefur verið ákveðið hvenær beri að rýna aðgangsheimildir að vefkerfinu? Æskilegt er að það sé gert að lágmarki árlega.	
Lykilorðastefna	
☐ Hafa lágmarkskröfur til lykilorða umsjónaraðila og notenda í veflausninni verið skilgreindar?	
☐ Ef svo er, er búið að virkja kröfur í samræmi við bestu starfsvenjur? Lengd lykilorða, líftími lykilorða, flækjustig (samblanda af hástöfum, bókstöfum, táknum), endurnýjun lykilorða.	
☐ Hafa lykilorð verið dulkóðuð í gagnagrunni veflausnar?	

Útfyllt af:	
Dags:	
Vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

UT-Vefhandbók

A.1.7.Gátlisti sem hægt er að nota við samningagerð

Gátlisti sem hægt er að nota við samningagerð. Helstu atriði er snerta öryggismál í samningagerð við þriðja aðila eru listaðir upp

Samantekt yfir atriði tengt samningagerð

Atriði	Athugasemdir
Innihald / viðmið	
☐ Inniheldur samningur ákvæði um hvaða þjónustuviðmið vistunaraðili skal inna af hendi (Service Level Agreement)? Þjónustuviðmið ættu að lágmarki að skilgreina með skýrum hætti hvaða þjónusta er veitt, uppitími lausnar, viðbragðstími, aðgengi að tæknimönnum og fleira.	
☐ Inniheldur samningur helstu atriði er snerta aðgang starfsmanna þjónustuaðila að gögnum verkkaupa?	
☐ Inniheldur samningur helstu kröfur um trúnaðarskyldu þjónustuaðila?	
☐ Innheldur samningur helstu kröfur um varðveislu og meðhöndlun á gögnum verkkaupa?	
☐ Inniheldur samningur yfirlit yfir allan þann véla- og hugbúnað sem samningur við þjónustuaðila nær yfir?	
☐ Ef utanaðkomandi aðila er veittur aðgangur að kerfum eða gögnum verkkaupa er tryggt að kröfur um trúnað og leynd séu uppfylltar? Með utanaðkomandi aðila er t.d. átt við aðila sem ekki er starfsmaður verkaupa eða þjónustuaðila.	
Eftirlit með samning	
☐ Hefur verið gert ráð fyrir reglubundum stöðufundum með þjónustuaðila í samningi?	
☐ Gerir samningur ráð fyrir frávikatilkynningu til verkkaupa ef þjónustuviðmiðum er ekki náð? Skilgreina ætti hvaða frávik eigi að tilkynna og hvernig skráning færi fram, slíkar frávikatilkynningar eiga að vera í samræmi við þjónustuviðmið.	
☐ Inniheldur samningurinn ákvæði um heimild verkkaupa til eftirlits með þeirri starfsemi þjónustuaðila sem samningurinn tekur til?	
☐ Hefur verið skilgreind heimild opinberra eftirlitsaðila um aðgang að gögnum og upplýsingum verkkaupa hjá þjónustuaðila?	
☐ Hefur verið skilgreindur eigandi og ábyrgðarmaður með samningnum, sem meðal annars hefur eftirlit með því að þjónusta sé í samræmi við þjónustuviðmið?	
Sérstök atriði	
☐ Ef um sérsmíði á lausn er að ræða, er höfundarréttur tryggður verkkaupa?	
☐ Hefur aðgengi að grunnkóða veflausnar verið tryggður ef verksali hættir starfssemi?	
☐ Eru ákvæði í samningum um að viðskiptavinir séu upplýstir um leið og öryggisgalli finnst sem notaður er í lausninni?	
☐ Ábyrgist þjónustuaðili öryggisuppfærslur að kostnaðarlausu?	
☐ Inniheldur samningur helstu kröfur um trúnaðarskyldu?	
☐ Innheldur samningur helstu kröfur um varðveislu gagna?	

Nánari upplýsingar er að finna í handbók um opinbera þjónustusamninga.

Útfyllt af:	
Dags:	
Vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

Gátlisti til að nýta við framkvæmd prófana á öryggi veflausna.Gátlisti er tæknilegur og krefst töluverðar þekkingar og tæknikunnáttu.

A.2.5 Gátlisti til að nýta við prófanir

Samantekt yfir atriði tengt prófunum

Atriði	Athugasemdir
Aðgangsstýring	
☐ Er stöðugt verið að framfylgja aðgangsstýringu óháð því hvort notandi hafi auðkennt sig? Dæmi um reikningsyfirlit: http://example.com/app/accountInfo?acct=notmyacct - Ef aðgangsstýring væri bundin við auðkenningu en væri ekki stöðugt framfylgt þá væri í þessu dæmi hægt að komast yfir reikningsyfirlit annara aðila.	
☐ Er meginreglum um lágmarksaðgang framfylgt? Þ.e.a.s. eru ákvarðanatökur byggðar á lágmarksréttindum? Er aðgangur almennt óheimilaður nema að hann sé sérstaklega leyfður?	
☐ Er þess gætt að ekki sé notuð bein tilvísun í vefhlut? Er aðgangi stýrt með tilliti til auðkenndra notenda og byggt á upplýsingum miðlaramegin? Sjá dæmi um reikningsyfirlit að ofan.	
☐ Eru notaðar ósannreyndar áframsendingar? Í einhverjum tilfellum getur verið nauðsynlegt að áframsenda notendur á aðrar síður t.d. ef reynt er að fara inn á síðu sem er ekki til. Passa þarf að óprúttnir aðilar geti ekki nýtt sér þetta eins og t.d. á eftirfarandi hátt: http://www.example.com/redirect.jsp?url=evil.com	
Auðkenning	
☐ Tryggja þarf að notendanöfn og lykilorð séu ekki harðkóðuð (skilgreind í forritunarkóða)	
☐ Tryggja að virkni við endursetningu lykilorða á veflausn sé útfærð á öruggan hátt. Ef notast er við öryggisspurningar, þá þurfa þær að vera erfiðar að giska á auk þess sem passa þarf upp á að ekki séu gefnar upplýsingar um hvort viðkomandi notandanafn sé til eða ekki.	
☐ Útfæra þarf læsingu aðgangs ef reynt er að skrá sig inn of oft (til þess að koma í veg fyrir e. „Brute force“ árásir). Hægt er að læsa aðgangi tímabundið. Hér er æskilegt að gefa sömu villuboð eins og þegar aðgangi er læst, rangt lykilorð er slegið inn og þegar að notandi er ekki til	
☐ Passa þarf að villuboð gefi ekki of mikið af upplýsingum. Á sama tíma og villuboð þurfa að vera skýr þá er æskilegt að þau gefi ekki upplýsingar um virk notendanöfn. Forðast ber að nota villuboð sem taka fram að lykilorð sé ekki rétt, það gefur í skyn að notandinn sé til. "Brute force" árásir ganga út á það að reyna mismunandi notendanöfn og lykilorð í þaula þangað til að aðgangi er náð að viðkomandi upplýsingakerfi.	
☐ Veflausn ætti að keyra með lágmarksréttindum. Hér ætti t.d. að takmarka aðgang veflausnarinnar við það sem hún þarf t.d. Les- og skrifaðgang, sem og aðgang að öðrum gögnum og gagnagrunnum sem ekki er þörf á.	
Inntaks og úttaksmeðhöndlun	
☐ Tryggja þarf að úttaksgögn séu kóðuð eftir samhengi áður en þau eru send til notenda. Það fer eftir staðsetningu í HTML kóða hvernig úttak er kóðað. T.d. þurfa gögn sem eru notuð í URL samhengi að vera kóðuð öðruvísi en gögn sem eru notuð í JavaScript samhengi. Dæmi: Ef gert er ráð fyrir því að taka við texta frá notanda sem verður birtur á annari síðu þá ætti ekki að leyfa sértákn sem væri hægt að nota í slæmum tilgangi eins og t.d. "<" og ">" í <script>alert("XSS");</script>	
☐ Nota á hvítlista fram yfir svartlista þegar verið er að taka á móti gögnum frá notendum. Hér er hægt að takmarka inntak einungis við þau tákn sem eru leyfileg. Hægt er að nota svartlista fyrir aukin sveigjanleika. Í stað þess að búa til svokallaðan svartan lista yfir sértákn sem eru ekki leyfð eins og ef við skoðum táknið "<", þá er hægt að tákna það á a.m.k. 70 mismunandi vegu. Hér eru nokkur dæmi: "<", "%3C", “&lt”, “<”, “&LT”, “<”, “&#60”, “&#060”, “&#0060” o.s.frv.	
☐ Passa þarf að nota (e.) Parameterized SQL queries til þess að verjast SQL innspýtingarárásum Dæmi um rétta leið (tekið frá OWASP): String custname = request.getParameter("customerName"); String query = "SELECT account_balance FROM user_data WHERE user_name = ? "; PreparedStatement pstmt = connection.prepareStatement(query); pstmt.setString(1, custname); ResultSet results = pstmt.executeQuery( );	
☐ Nota ætti tákn (e. Token) á vefsíðum til þess að koma í veg fyrir (e.) Cross Site Request Forgery (e. CSRF) Dæmi um CSRF veikleika (tekið frá OWASP): Til þess að fyrirbyggja CSRF árásir ætti að nota óútreiknanlegt token í hverri HTTP fyrirspurn. Slík token ættu í það minnsta að vera einkvæm fyrir hverja notendalotu.	
☐ Passa þarf að innsendar skrár séu sannreyndar. Sannreyna á stærð, tegund, innihald auk þess sem gæta þarf þess að ekki sé hægt að hafa áhrif á hvar skráin er vistuð á miðlara.	
☐ Nota ætti nosniff hausinn: Content-Type-Options: nosniff Sjá nánari upplýsingar um nosniff hausinn: https://www.owasp.org/index.php/List_of_useful_HTTP_headers	
☐ Nota ætti X-Frame-Options til þess að sporna gegn click-jacking árásum	

- [ ]

Sjá nánari upplýsingar um X-Frame-Options hausinn: https://www.owasp.org/index.php/List_of_useful_HTTP_headers

- [ ] Nota ætti CSP eða X-XSS protection til þess að sporna gegn endurspegluðum XSS árásum

Sjá nánari upplýsingar um CSP og X-XSS hausana: https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Lotustjórnun

- [ ] Tryggja þarf að Session Identifiers séu nægjanlega óútreiknanlegir (sufficiently random) þannig að árásaraðilar geti ekki giskað á þá og tekið yfir lotu annarra.
- [ ] Eru lotutákn (e. Session Identifier) endurnýjuð? T.d. eftir auðkenningu eða eftir að skipt er milli dulkóðaðra samskipta yfir í ódulkóðuð samskipti eða öfugt
- [ ] Er búið að útfæra sjálfvirka útskráningu notenda sem hafa ekki verið virkir í einhvern tíma?
- [ ] Er lotunotanda lokað ef einhver merki eru um hagræðingu eða svik (e.tampering)?
- [ ] Er lota ógild eftir að notandi hefur skráð sig út?
- [ ] Er útskráningartakki á hverri síðu?
- [ ] Er búið að virkja örugga vafrakökuþætti (e. Cookie attributes) (Httponly and Secure Flags)

Sjá nánari upplýsingar: https://www.owasp.org/index.php/SecureFlag

- [ ] Er búið að stilla vafraköku lén (e. cookie domain) og slóð (e. path) rétt

Sjá nánari upplýsingar: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

- [ ] Er búið að skilgreina endingartíma á vafraköku? Forðast á vafrakökur sem hafa ekki skilgreind gildislok.

Sjá nánari upplýsingar: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Verndun gagna

- [ ] Er SSL dulkóðun notuð alls staðar? Ef ekki er mögulegt að nota SSL alls staðar skal nota SSL á öllum staðfestingarsíðum ásamt þeim síðum þar sem notendur auðkenna sig.

SSL (Secure Socket Layer) er dulkóðunar samskiptastaðall. Hægt er að nota SSL til þess að dulkóða ýmis samskipti, meðal annars vefumferð (Hyper Ttext Transfer Protocol), þá er talaða um HTTPS (Hyper Text Transfer Protocol Secured).
TLS (Transfer Layer Security) er dulkóðunar samskiptastaðall sem hefur tekið við af SSL.

- [ ] Er búið að gera HTTP aðgang óvirkan fyrir alla virkni veflausnarinnar sem á að fara yfir SSL/TLS?
- [ ] Er (e.) „Strict-Transport-Security“ hausinn notaður?

Sjá nánari upplýsingar: https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

- [ ] Eru lykilorð vistuð með því að nota nokkrar ítranir af öruggu tætifalli af því ásamt slembigögnum (e. Salt)?
- [ ]

Ef veflausn styðst við/notar dulkóðun, hefur hún þá verið útfærð á þann veg að hún tryggi örugg skipti á dulkóðunarlyklum?

- [ ] Ef dulkóðunarlyklar eru notaðir, er búið að skilgreina sýslunarferli fyrir dulkóðunarlyklana til þess að takmarka aðgang að þeim?
- [ ] Er búið að óvirkja stuðning við veika dulkóðunarmöguleika yfir SSL?
- [ ] Eru rafræn skilríki sem notuð eru við SSL samskipti gefin út af traustum aðilum (e. Trusted certificate authority)?
- [ ] Er búið að óvirkja geymslu gagna í flýtiminni (e. Data caching) með því að nota HTTP hausa eða metatag?
- [ ] Er búið að takmarka notkun og geymslu viðkvæmra gagna.

Villumeðhöndlun og atvikaskráning

- [ ]

Er einungis birt almenn villuskilaboð? Þ.e.a.s. án þess að birta smáatriði um innra ástand hugbúnaðarins (e. Application)?

- [ ] Er þess gætt að allar undantekningar (e. Exception) séu meðhöndlaðar?
- [ ] Er passað upp á að gefa ekki upp viðkvæmar upplýsingar við villumeldingar?
- [ ] Eru allar auðkenningar (e. Authentication activities) skráðar (e. Log) sama hvort þær heppnist eður ei?
- [ ] Eru allar breytingar á réttindum skráðar (e. Log)? T.d. ef réttindastig notanda breytist ætti að skrá það.
- [ ] Eru allar stjórnunarbreytingar (e. Administrative changes) skráðar (e.Log)?
- [ ] Er allur aðgangur að viðkvæmum gögnum skráður (e. Log)? Þetta á sér í lagi við stofnanir sem þurfa að hlíta ákveðnum stöðlum um öryggi og meðhöndlun gagna
- [ ] Er þess gætt að óviðeigandi gögn séu ekki skráð? Gögn sem flokkast sem óviðeigandi gögn eru t.d. viðkvæm gögn (e. Sensitive data)
- [ ] Eru skráningar (e. Logs) geymdar á öruggan hátt og þannig komið í veg fyrir gagnatap eða breytingar af hálfu tölvuþrjóta?

Útfyllt af:	
Dags:	
Vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

Gátlisti fyrir örugga hönnun á veflausn s.s. ferli við kóðun, rýni, prófanir o.fl.

UT-Vefhandbók

A.6.3 Gátlisti fyrir örugga hönnun á veflausn

Samantekt yfir atriði tengt öruggri hönnun

Atriði	Athugasemdir
Örugg hönnun á veflausn	
☐ Hefur hugbúnaðarþróunarferli verið skilgreint?	
☐ Hefur regluverk við forritun verið skilgreint?	
☐ Hefur formfast breytingarstjórnunarferli verið skilgreint og skjalað sem m.a. tekur tillit til prófana og öryggisþátta?	
☐ Hafa öryggiskröfur veflausnar verið skilgreindar?	
☐ Hefur ábyrgð verið úthlutað við framkvæmd öryggisúttektar á hönnunarferlinu til þess að aðstoða við að innleiða viðeigandi gagnráðstafanir inn í ferlið?	
☐ Hefur ábyrgð við framkvæmd rýni á kóða verið úthlutað með tilliti til öryggis? Reglulega þarf að fara yfir kóða í leit að almennum vandamálum eins og SQL innspýtingu og Cross-Site Scripting. Þetta ætti að vera hluti af breytingastjórnunarferli	
☐ Hefur ferli við meðhöndlun frávika sem upp koma við hugbúnaðarþróun og breytingar verið skilgreint?	
☐ Hafa forritarar hlotið þjálfun í öruggri hugbúnaðarþróun? (sjá gátlista í kafla 2.5 um prófanir á öryggi veflausna)	

Útfyllt af:	
Dags:	
Vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

Gátlisti fyrir örugga uppsetningu á stýrikerfum, netþjónum og gagnagrunnum sem hýsa veflausn

UT-Vefhandbók

A.6.3 Gátlisti fyrir örugga uppsetningu grunnkerfa

Samantekt yfir atriði tengt öruggri uppsetningu

Atriði	Athugasemdir
Grunnkerfi	
☐ Hefur ábyrgðarmaður verið skráður á póstlista fyrir öryggisuppfærslum þeirra kerfa sem notuð eru?	
Sem dæmi um kerfi má nefna: Stýrikerfi, gagnagrunnur, netbúnaður, stuðningshugbúnaður o.fl.	
☐ Hefur verið skilgreint formlegt ferli sem tryggir að brugðist sé við þegar að nýjar öryggisuppfærslur eru gefnar út?	
Æskilegt er að brugðist sé við innan þriggja daga frá því að öryggisuppfærslur eru gefnar út	
☐ Hefur verið lokað fyrir allar þjónustur og port á kerfum sem ekki er verið að nota?	
☐ Hefur verið farið yfir notendalista og lokað fyrir lykilorð sjálfgefinna notenda eða þeim breytt?	
☐ Hefur verið staðfest að villumeldingar og atvikaskrár gefi ekki upp viðkvæmar upplýsingar til notenda?	
Til dæmis notendanöfn, kennitölur, kortaupplýsingar eða aðrar viðkvæmar upplýsingar	
☐ Er til staðar öryggisbúnaður s.s. eldveggur eða innbrotsvöktunarkerfi?	
☐ Hefur aðgangur að kerfum verið takmarkaður eins og kostur er?	
Sem dæmi um kerfi má nefna: Stýrikerfi, gagnagrunnur, netbúnaður, stuðningshugbúnaður o.fl.	
☐ Hafa viðeigandi ráðstafanir verið gerðar til varnar vírusum og óværu á miðlara?	