



Upplýsingar um gátlista

Gátlistinn er hugsaður sem tól til að aðstoða vefstjóra við örugga hönnun veflausnar, hvort sem er frá þriðja aðila eða við eigin hönnun veflausnar. Í gátlistanum er að finna upplýsingar um hvað helst ber að hafa í huga þegar kemur að útfærslu öryggisþátta í veflausn.

Gátlistinn er ekki tæmandi og er eingöngu hugsaður sem tól sem vefstjórar geta leitað í þegar til stendur að kaupa, þróa eða uppfæra veflausnir og vefsíður viðkomandi stofnunnar.

Ekki er ætlast til að vefstjórar búi yfir þekkingu á öllum þeim atriðum sem koma fram í gátlistanum.

Gátlistinn styður við kafla 6.2. Öryggi veflausna í UT handbókinni.

Ef vefstjórar nota gátlistann er gott að setja inn athugasemdir þar sem við á og vista eintak af gátlistanum til uppfléttingar.



INNANRÍKISRÁÐUNEYTIÐ

UT-Vefhandbók

A.6.3 Gátlisti fyrir örugga hönnun á veflausn

Útfyllt af:	
Dags:	
Vefsvæði / lén:	

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



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)