



Hvað er rétt að vefstjórar séu
að gera í öryggismálum?



Öryggismál eru svo leiðinleg



Öryggismál eru svo leiðinleg



Þurfum smá heilapvott

Hugarfarsbreytivél í gangi



6 ráð fyrir vefstjóra

Ráð #1: Þekktu mótherjann

Ráð #2: Meta þörf eftir aðstæðum

Ráð #3: Öðlaðstu þekkingu og leitaðu ráða

Ráð #4: Gerðu kröfur

Ráð #5: Notaðu öryggi sem tækifæri

Ráð #6: Koma ábyrgð til skila

Ráð #1: Þekktu mótherjann

Staðreynd #1:

Hann er ekki vinur þinn



Ráð #1: Þekktu mótherjann

Staðreynd #2:

Það er oft brotist inn og breytt vefjum á Íslandi



Ráð #1: Þekktu mótherjann

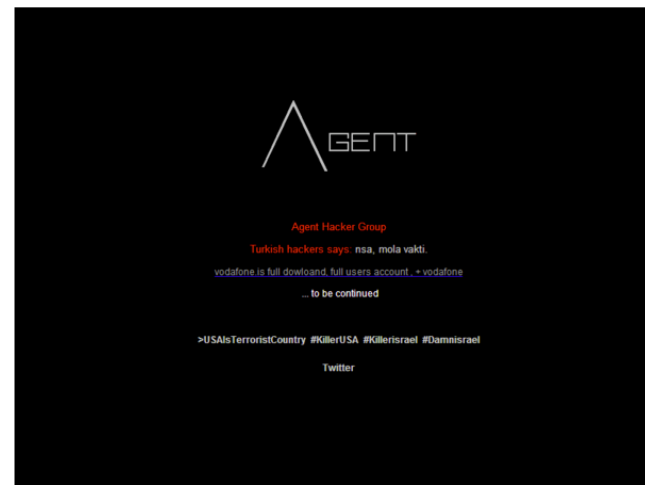
Staðreynd #3:

Fólk tekur vefinnbrot ekki alvarlega nema þeir geri eitthvað með aðganginn



Official Vodafone Iceland hacked and defaced with 77,000 accounts leaked

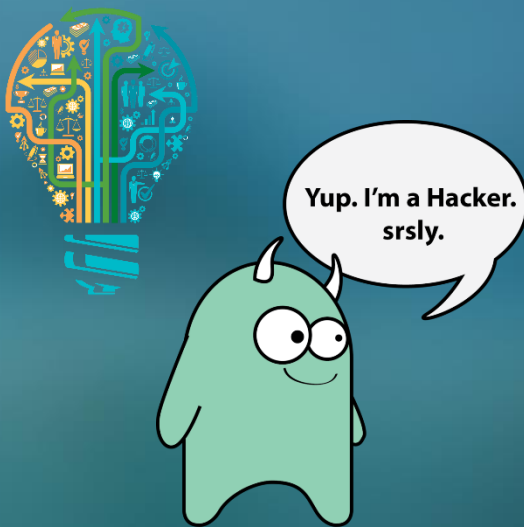
Published November 30th, 2013 By Lee J



Ráð #1: Þekktu mótherjann

Staðreynd #4:

Það er mjög stutt stökk milli þess að breyta vef og nýta sér allt sem hann hefur aðgang að



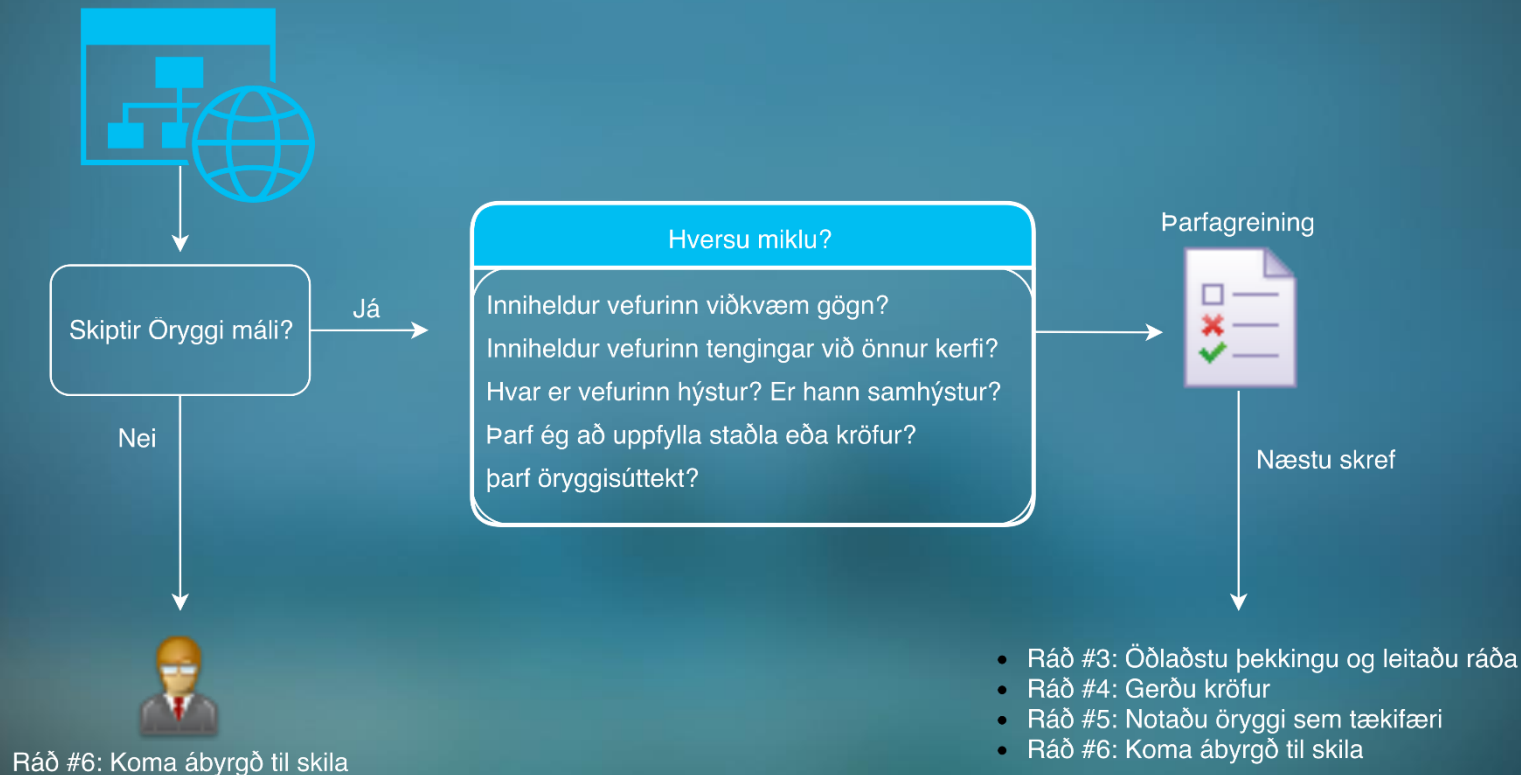
Ráð #1: Þekktu mótherjann

Staðreynd #5:

Atvik þar sem gögn leka geta haft mjög alvarlegar afleiðingar



Ráð #2: Meta þörf eftir aðstæðum



Ráð #3: Öðlastu þekkingu og leitaðu ráða

Byrjaðu að fræðast um OWASP “Open Web Application Security Project”

“The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.”

Notaðu þér það efni sem til er

t.d: <http://www.ut.is/vefhandbok/yfirlit/oryggi/>



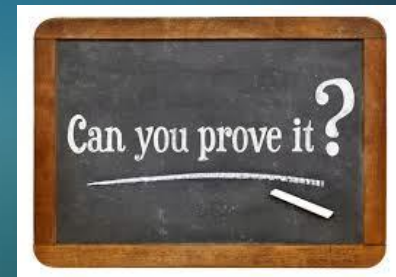
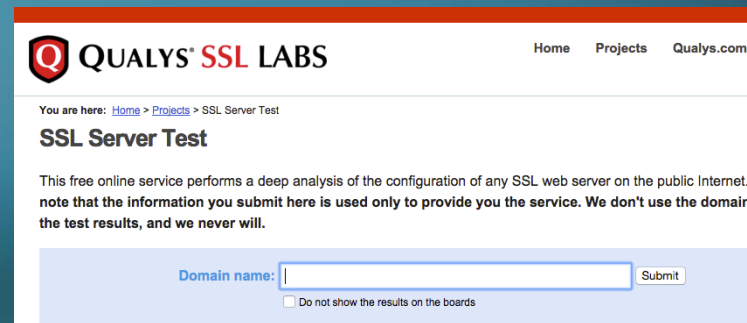
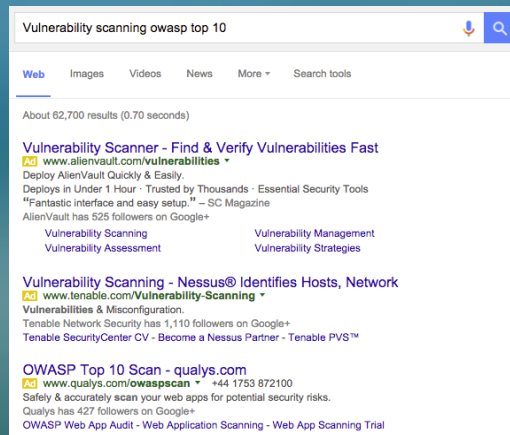
Ráð #3: Öðlastu þekkingu og leitaðu ráða

Ekkert kerfi/umhverfi/vefur er eins og það þarf að meta stig og nauðsyn öryggis miðað við aðstæður



Ráð #3: Öðlastu þekkingu og leitaðu ráða

Ekki treysta í blindni og fáðu óháð ráð. Treystu bara því sem fólk getur sannað og þar sem áhrifin eru skiljanleg



Ráð #4: Gerðu kröfur

- Þjónustuaðilar og hugbúnaðarhús
 - Láttu Öryggi skipta miklu máli við val á birgja/þjónustuaðila
 - Hvað eru þeir að gera í öryggismálum?
 - Góð regla er að fá álit á þeirra svörum!



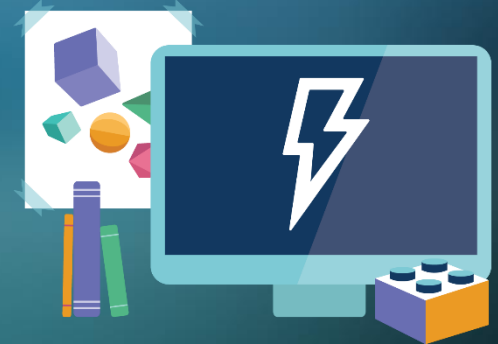
Ráð #4: Gerðu kröfur

- Vefur sem krefst öryggis á ekki að vera í samhýstu vefumhverfi
 - Veikasti hlekkurinn bitnar á öllum
 - Þarf ekki endilega að kosta mikið meir



Ráð #4: Gerðu kröfur

- Hafa þróunaraðilar fengið fullnægjandi þjálfun?
 - Þekkja þeir öryggisveikleika? (OWASP topp tíu) ?
 - Vita þeir hvernig á að komast hjá veikleikunum?
 - Hvernig bregðast þeir við öryggisveikleikum?



Ráð #4: Gerðu kröfur

- Gerðu kröfu um öryggismál í samningum
 - Þurfið þið að borga fyrir öryggisuppfærslur?
 - Gerið þið kröfu um að þjónustuaðilar og þróunaraðilar láti vita af atvikum og veikleikum?



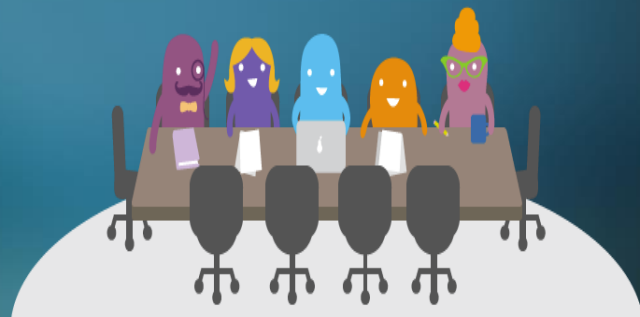
Ráð #5: Notaðu öryggi sem tækifæri

- Tækifæri til að aðgreina sig frá samkeppninni
- Notendum langar að líða eins og hlutirnir séu í lagi og öruggir
 - Passa sig bara á að ímynd != öryggi
- Hvernig er hægt að nota öryggi til þess að auka aðgengi og þægindi notenda?



Ráð #6: Koma ábyrgð til skila

Hver ber ábyrgð ef allt fer til fjandans og hvaðan eiga peningarnir að koma? Hver er ábyrgð vefstjórans?





syndis.is