ÓSKÖPUM LAUMAÐ INN Í HUGBÚNAÐ („SQL INJECTION“)

2017 ÖRYGGI UPPLÝSINGAKERFA HINS OPINBERA

8. Mars 2017

Svavar Ingi Hermannsson,
CISSP, CISA, CISM

ÓSKÖPUM LAUMAÐ INN Í HUGBÚNAÐ („SQL INJECTION“)

- Hvað er SQL injection?
- Hvernig verða SQL injection veikleikar til?
- Hvaða áhrif hefur þetta á okkur?
- Hvað getum við gert til þess að vernda okkur gegn SQL injection árásum?

SECURITY.IS

HVAÐ ER SQL INJECTION

- Dæmi um gagnadrifin forrit eða vefsíður
  - Símaskrá
  - Amazon
- Hvað er SQL (Structured Query Language)?
  - statement = "SELECT * FROM users WHERE name = '" + userName + "';”
- Hvað er SQL injection?
  - userName = "test'; insert into users values(1, ’newadmin', ’lykilord', 9)/*"

SECURITY.IS

HVERNIG VERÐA SQL INJECTION VEIKLEIKAR TIL?

- Forritarar hafa oft ekki næga þekkingu í öruggri hugbúnaðarþróun
  - Öryggi í hugbúnaðarþróun ekki skyldu áfangi í háskólanámi
- Aukin áhrif
  - Aðgangur að upplýsingakerfum oft ekki rétt stýrður
    - Admin aðgangur að gagnagrunni eða gagnagrunnsmiðlara í staðin fyrir les aðgang að einni töflu.

SECURITY.IS

HVAÐA ÁHRIF HEFUR ÞETTA Á MIG?

- Global Threat Intelligence Report (GTIR) - 2014
  - SQL injections cost $196,000
- Sony's Hacking Scandal Could Cost The Company $100 Million – Business Insider UK 2014
- Microsoft Advanced Threat Analytics (ATA) playbook - 2017
  - "The average cost of a cyber intrusion is estimated to be around $3.8M for an enterprise, per incident."
- Panama lekinn
  - Drupalgeddon?
  - Wordpress Plugin

SECURITY.IS

HVAÐA ÁHRIF HEFUR ÞETTA Á MIG?

- Attack surface
  - Eru einhver ytri kerfi sem eru beintengd við gagnagrunna?
- Er verið að nota upplýsingakerfi frá þriðja aðila sem tengist gagnagrunnum með SQL?
  - Drupal?
  - Wordpress?
  - Önnur vefkerfi?
  - Heimatilbúin forrit?

HVAÐ GETUM VIÐ GERT TIL ÞESS AÐ VERNDA OKKUR?

- Setja inn öryggisuppfærslur reglulega
- Fara fram á að fá tilkynningar um öryggisveikleika sem finnast í hugbúnaði
- Þjálfa starfsfólk í að skrifa öruggan kóða
- Gera kröfu á birgja um formlegt og öruggt hugbúnaðarþróunarferli
- Öryggisúttektir
- Veracode / Checkmarx o.fl.
- WAF (Web Application Firewall)
- Intrusion Prevention System (IPS)

SECURITY.IS

TAKK FYRIR

- Einhverjar spurningar?

svavar@security.is

SECURITY.IS