BITI

Ēriks Dobelis, BITI

Tīmekļa vietņu drošība

Interneta lietojumu vietņu drošības aktualitāte

- 100tiem vietņu tiek uzlauztas ikdienā
  - CERT.LV var Jums pastāstīt…
  - http://www.zone-h.org/
  - Google, Microsoft, Oracle, Amazon – visiem ir «vēsture»
- Drošas programmēšanas pamatiemaņu trūkums
- Augsta publicitāte, neskatoties uz bieži zemu ietekmi
- Hakeru komercializēšanās
- Budžeta ierobežojumi
- Interneta lietojumi – nākotnes izstrādes vide

BITI

Ko var darīt?

- Veidot labas ārējās un iekšējās attiecības ##
- Noteikt drošības prasības
- Programmēt droši
- Administrēt droši
- Testēt drošību
- Veidot drošu arhitektūru
- Uzraudzīt drošību

BITI

Labas ārējās un iekšējās attiecības

- Attiecībā uz mājas lapu drošību – viens no būtiskākajiem aspektiem
- Kāpēc www.vdi.gov.lv uzbrūk vairāk nekā, piemēram, www.dabasmuzejs.gov.lv ?

Drošības prasības

- Drošības prasības ir nefunkcionālās prasības
- Pasūtot izstrādi par tām visbiežāk vai nu aizmirst, vai uzskata par pašsaprotamām
- Negatīvās prasības (sistēma nedrīkst uzvesties tā... nevis sistēma darīs tā...)
  - Grūti noformulēt
  - Grūti dot konkrētu programmēšanas uzdevumu
  - Grūti pārliecināties par piegādi
- Bez drošības prasībām nav drošas izstrādes!

BITI

Programmēt droši

- Diemžēl universitātēs pie mums to nemāca

- Projektu vadītāji un pasūtītāji prioritizē funkcionālās prasības (jo tās var pārbaudīt)
- OWASP
  - The Open Web Application Security Project
  - www.owasp.org
  - Būtiskāko Interneta lietojumu drošības problēmu apkopojums

BITI

OWASP Top 10

A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2-Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A3-Broken Authentication and Se	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
A4-Insecure Direct Object Referer	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5-Cross Site Request Forgery (CS	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A6-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.
A7-Insecure Cryptographic Storag	Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.
A8-Failure to Restrict URL Access	Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.
A9-Insufficient Transport Layer Pr	Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.
A10-Unvalidated Redirects and Fo	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

BiTI

Administrēt droši

- Spiediens no gala pasūtītāja un izstrādātāja
- Standarta produktu jauninājumu uzstādīšana
  - Riskēt sagraut funkcionalitāti vai riskēt atstāt caurumu?
- Izstrādātāju nošķiršana no ekspluatācijas vides
  - Administratora mugurkaula stingrums
  - Samazina produktivitāti (bet arī riskus)

BITI

Testēt drošību

- Specifiska testēšanas joma
- Izstrādātāji un testētāji ar to nenodarbojas
- Testēšanai arī ir savs risks – nevar iegūt 100% garantiju, ka nav drošības problēmu
- Pie nākamās izmaiņas konfigurācijā var atklāties caurums, kura pirms tam nebija
- Tuvu nereālam atklāt speciāli veidotu caurumu
- Pastāvīgi tiek atklāti principiāli jauni ievainojamību veidi
- Pilna pirmkoda drošības analīze – ĻOTI dārgi

BITI

Veidot drošu arhitektūru

- Lielo organizāciju IS arhitektūra ir kļuvusi ļoti sarežģīta – neviens to kopumā nepārzin
- Interfeisu daudzums ar citām iestādēm arī nepalīdz
- Interneta lietojumu ievainojamības «apiet» daudzas tradicionālās drošības kontroles
- Masveidā notiek paļaušanās uz to, ka uzprogrammēts ir 100% droši

BITI

Uzraudzīt drošību

- Standarta IDS rīki labi strādā tikai pret standarta uzbrukumiem
- Prasa lielu laika ieguldījumu caurskatīt lielu auditācijas pierakstu apjomu
- Prasa profesionalitāti izvērtēt uzbrukumu nopietnību
- Bez adekvātiem auditācijas pierakstiem nav iespējams veikt analīzi pēc uzbrukuma
- Bet nekas nevar būt sliktāk kā konstatēt, ka uzbrucējs jau pusgadu ir nepamanīts

BITI

Kopsavilkums

- Ja sistēmai ir 5 interfeisi un katrs no tiem ir 90% drošs, cik droša ir sistēma?
- Nevar paļauties tikai uz viena veida aizsardzību – katrai ir savi trūkumi, bet katra spēlē savu nozīmīgu lomu kopējā drošībā

BITI