

Rails drošība

Biežākās web aplikāciju drošības problēmas

- Sesiju “nolaupīšana”
- Cross-Site Request Forgery
- Cross-Site Scripting (XSS)
- vājas paroles
- SQL injekcija
- Apzināti sabojāti ievaddati

Rekomendētās Ruby on Rails tehnikas

Modeļi

attr_accessible attr_protected	Aizsargā kritiskos atribūtus no masveida piešķiršanām
? parametri SQL komandās	Nevajag izmantot virkņu apvienošanu vai #{...}
validācijas ievadīto datu pārbaudei	Nedrīkst paļauties uz HTML formu validācijām

Kontrolieri

privātās metodes	Visām metodēm, kas nav darbības (action) jābūt privātām, vai jāizmanto <code>hide_action</code>
<code>before_filter</code>	Autorizācijas nodrošināšanai
nav SQL pieprasījumi	Jebkādi SQL pieprasījumi jāpārviesto uz modeļiem
<code>params[:id]</code>	Jāpārbauda id derīgums un vai lietotājam ir pieeja šim ierakstam

Kontrolieri

hidden fields	Jāuzmanās no apslēpto lauku vērtībām, nedrīkst izmantot pieejas tiesību ierobežošanai
filter_parameter_logging	Ierobežo, kādi parametri neparādās log failā
jāstrādā bez skatījumiem	Testējot drošību, jāiedomājas, ka nav skatījumu un kontrolieri var saņemt jebkādus datus
GET / POST pareiza apstrāde	Ar GET pieprasījumiem neveikt bīstamas darbības – dzēšanu, labošanu

Skatījumi

h	Visi lietotāju ievadītie dati jāattēlo ar h helperi vai WhiteListHelper
	Tas pats arī jāņem vērā AJAX pieprasījumu rezultātu ģenerēšanā
neatstāt komentārus	Skatījumos nevajag atstāt komentārus, ko negrib, ka visi redz

Sesijas

SSL	<code>ActionController::Base.session_options[:session_secure] = true</code>
sesiju uzturēšana	<code>reset_session</code> <code>session[:user_id] = nil</code>
autentifikācija	Vēlams izmantot standarta plug-inus, kā <code>restful_authentication</code>
sesiju derīguma termiņš	Neaktīvu / visu sesiju izbeigšana pēc noteikta termiņa, atkārtota autentifikācija

Paroles

šifrētas paroles datubāzē	Digest::SHA1.hexdigest restuful_authentication
labas paroles	validates_format_of validates_length_of
nesaglabāt log failos	filter_parameter_logging "password"

Informācijas avoti

- <http://www.rorsecurity.info>
- http://www.railsconfeurope.com/presentations/railsconfeurope07/re7_webbers.ppt