# **Defending against SQL-injections**



#### Defending against SQL-injections

- Application level defenses
  - Sanitazing user input
    - F.e. PHP addslashes(), mysql\_real\_escape()...
  - Using IDS-software components like PHPIDS
- Intrusion Detection Systems
  - Monitors network traffic for fingerprints of know vulnerabilities
- Web Application firewalls
  - Inspects HTTP traffic for web server
  - Blocks malicius traffic and logs them



### Web Application Firewall location

- In general WAF can be located at
  - Between the webserver and the client
    - Dedicated hardware
  - Integrated into webserver
    - Software component
  - Connected to a switch trough port mirror
    - Dedicated hardware or switch component



#### Application level defenses

- White listing
  - Allowing only input that is specific for the input
  - F.e. if the input is numeric only numerical values are allowed
  - Effective and produces less false positives
  - Hard to implement since all cases has to be considered
- Black listing
  - Filtering certain keywords from user input
  - Easy to implement
  - Easy to evade if not properly implemented



### **Evading filters**

- URL encoding to evade filter pattern matching
  - Is "effective" against WAFs which are filtering HTTP traffic
  - Will not work against application level protections since the input is url-decoded by webserver ->application will receive urldecoded message



# Keyword filtering

- Removing database keywords from input
  - SELECT, UNION, WHERE, OR and so on
- Question arises what you can remove?
  - Depends on the input
  - Discussion group message:
    - Please select correct version of a software and ...



# Keyword filtering

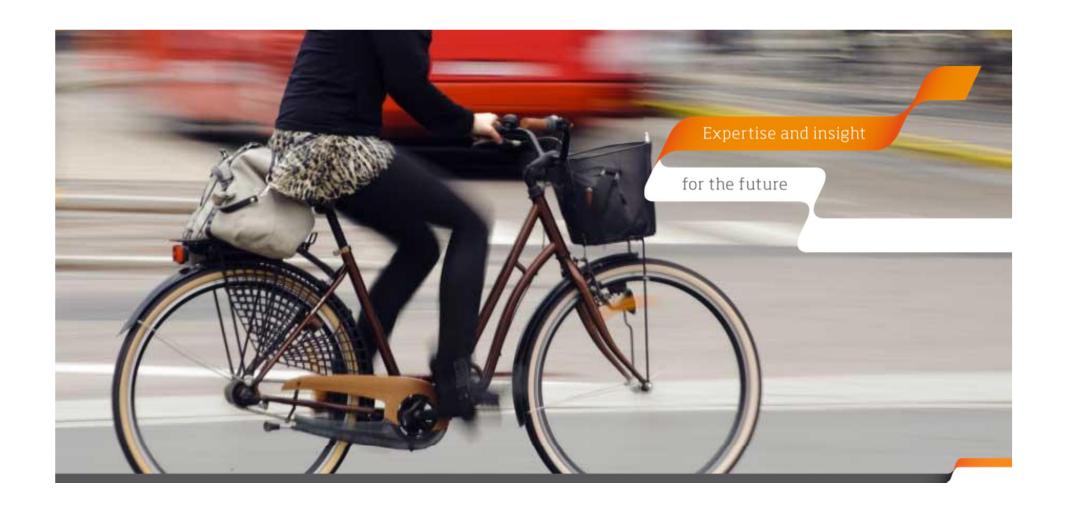
- 'AND' and 'OR' filtered by WAF
  - Easy to replace with && and ||
- 'SELECT' filtered
  - Lower and upper case mixes might fool very simple filters f.e. 'SeLeCt'
  - Otherwise quite hard since keywords can't really be obfuscated
    - Mysql SEL/\*\*/ECT does not work after version 4.1.



# Keyword filtering

- Filtering 'UNION SELECT'
  - Easy to bypass, basically anything added between the control words breaks the filter
  - 'union /\*!select\*/ pass from users#
- Filtering 'UNION'
  - Can be evaded using blind injection





#### THANK YOU!

www.metropolia.fi/en/ www.facebook.com/MetropoliaAMK kimmo.sauren@metropolia.fi

