Web Security and the OWASP Top 10: The Big Picture

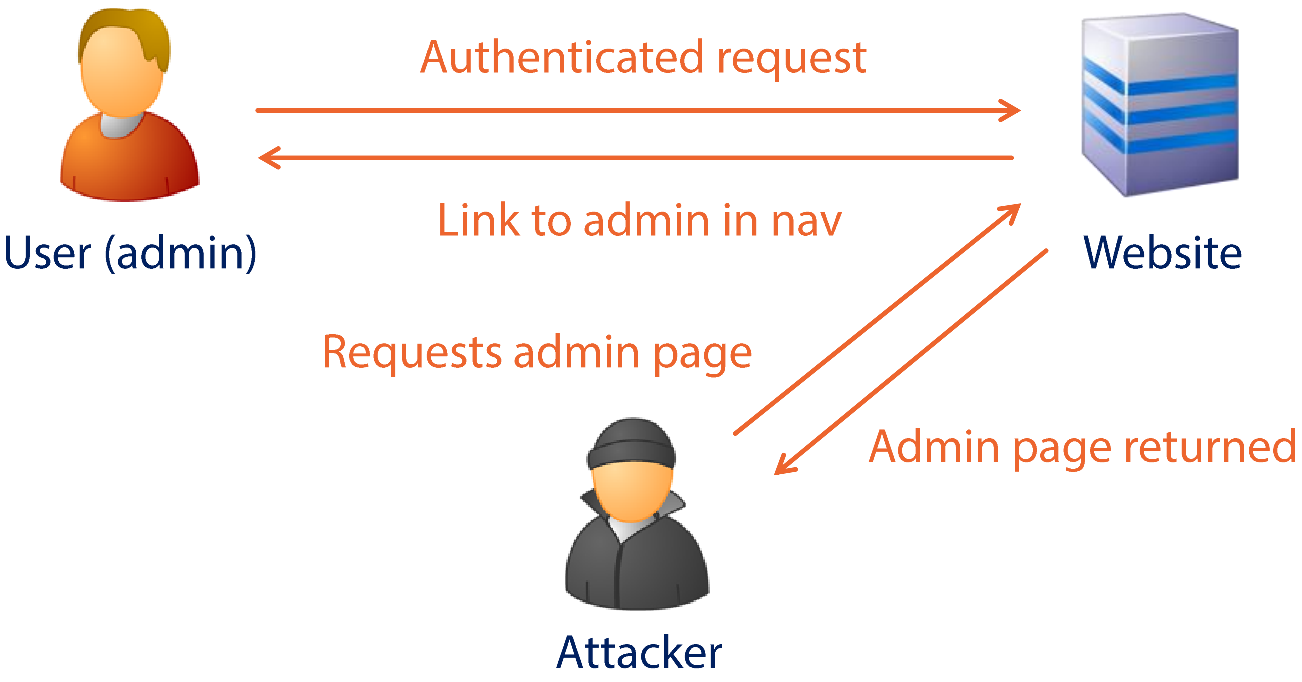
Missing Function Level Access Control

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Missing Function Level Access Control

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Easy	Prevalence Common	Detectability Average	Impact Moderate



Authenticated request

Link to admin in nav

User (admin)

Website

Requests admin page

Admin page returned

Attacker

Understanding Missing Function Level Access Control

- Does the UI show navigation to unauthorised functions?
- Are server side authentication or authorisation checks missing?
- Are server side checks done that solely rely on information provided by the attacker?
- Are system or diagnostic resources accessible without proper authorisation?
- Will “forced browsing” disclose unsecured resources?

Common Defences Against Missing Function Level Access Control

Define a clear authorisation model

- Define centrally and consistently
- Use roles and apply membership

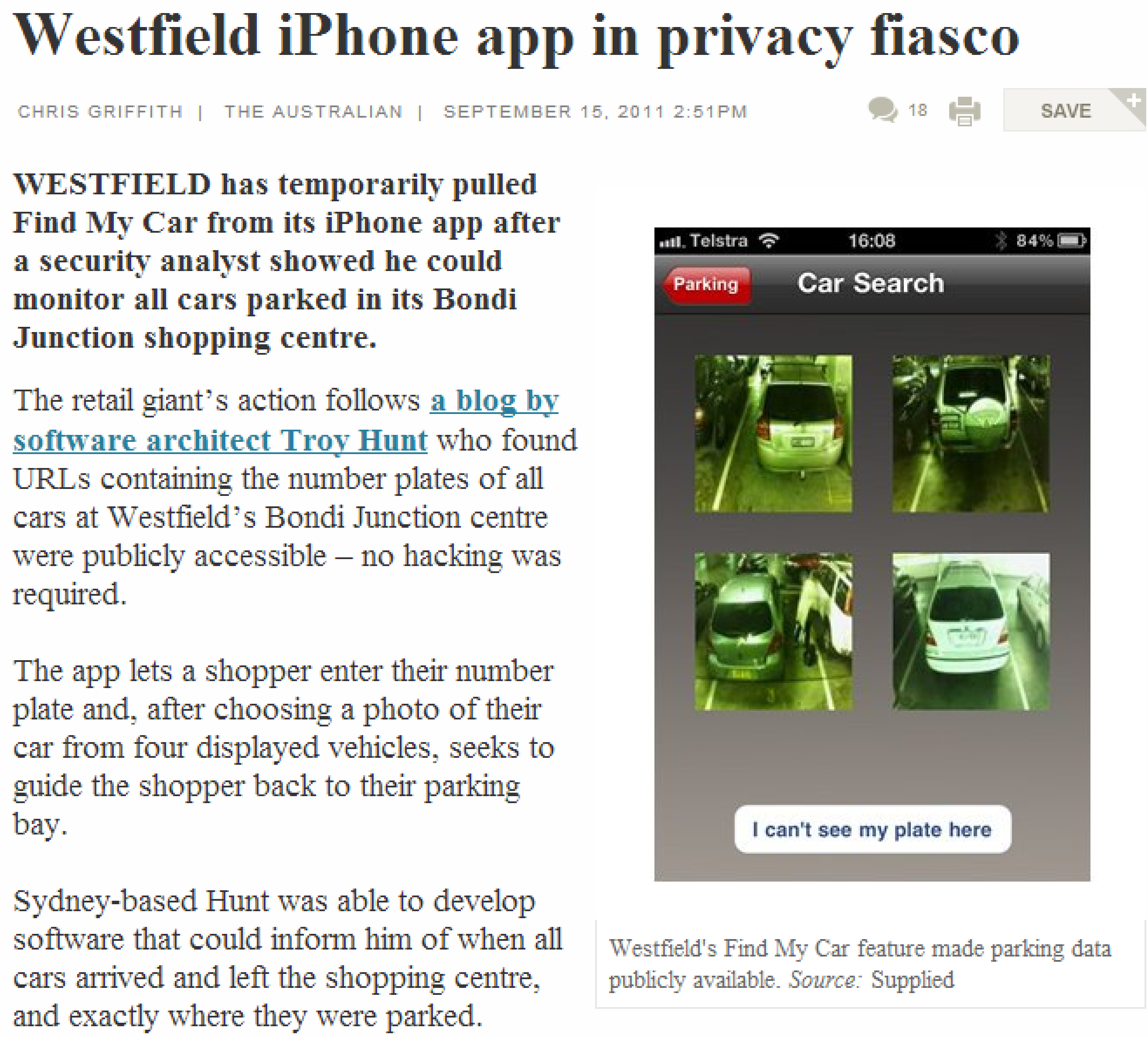
Check for forced browsing

- Check for default framework resources
- Automated scanners are excellent for this

Always test unprivileged roles

- Capture and replay privileged requests
- Include POST requests and async calls

Missing Access Controls in the Wild – Westfield



Westfield iPhone app in privacy fiasco

CHRIS GRIFFITH | THE AUSTRALIAN | SEPTEMBER 15, 2011 2:51PM

18

SAVE

WESTFIELD has temporarily pulled Find My Car from its iPhone app after a security analyst showed he could monitor all cars parked in its Bondi Junction shopping centre.

The retail giant's action follows a blog by software architect Troy Hunt who found URLs containing the number plates of all cars at Westfield's Bondi Junction centre were publicly accessible – no hacking was required.

The app lets a shopper enter their number plate and, after choosing a photo of their car from four displayed vehicles, seeks to guide the shopper back to their parking bay.

Sydney-based Hunt was able to develop software that could inform him of when all cars arrived and left the shopping centre, and exactly where they were parked.

Westfield's Find My Car feature made parking data publicly available. *Source:* Supplied