

SECURITY TESTING HANDS ON AS MOB TESTING

DANIEL BILLING

MAARET PYHÄJÄRVI

A solid blue horizontal bar at the bottom of the slide.

INTRODUCTIONS



MAARET

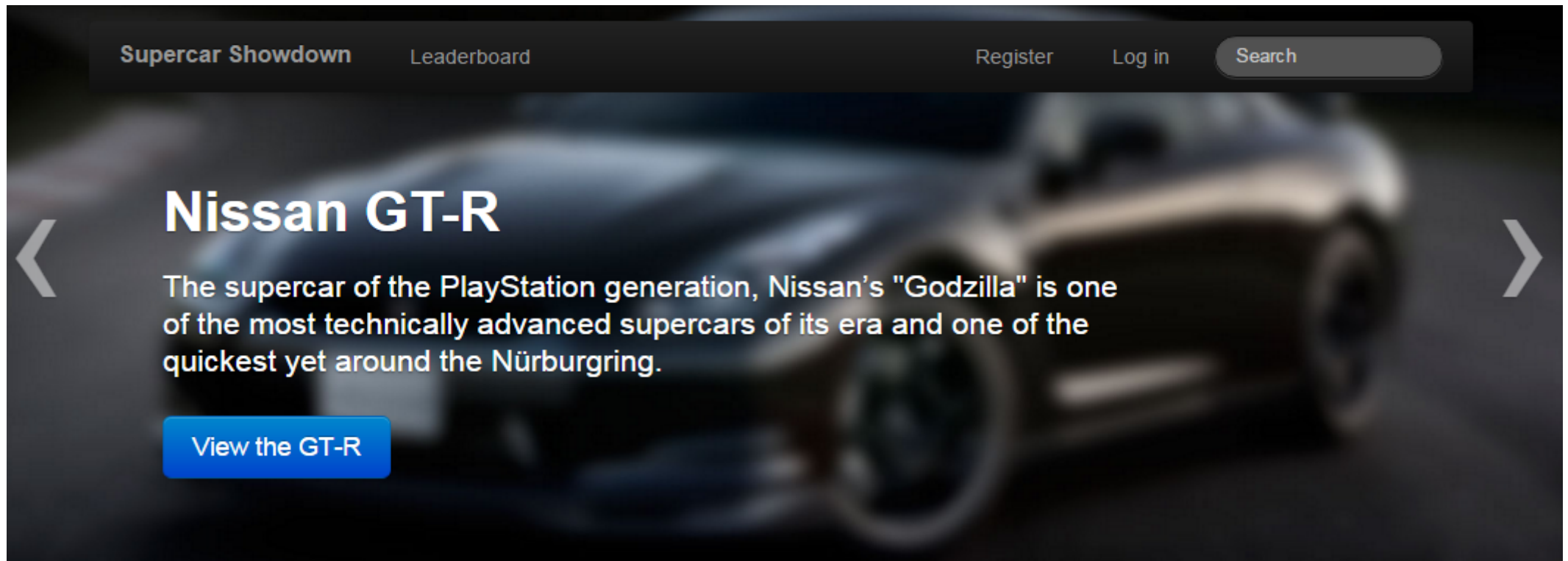


DAN

WHAT ARE WE TESTING?

<http://hackyourselffirst.troyhunt.com/>

BY TROY HUNT @troyhunt



SECURITY TESTING! WHAT IS IT?

ITS LIKE **ANY OTHER** KIND OF TESTING EXCEPT WITH SECURITY, INTEGRITY OF USER AND SYSTEM DATA AT ITS FOCUS

DON'T BE AFRAID

TRY **NEW** THINGS

THINK ABOUT **HEURISTICS** IN SECURITY – PRIVACY, AUTHENTICATION, AUTHORISATION

THINK ABOUT COMMON **VULNERABILITIES** – OWASP TOP 10 AND MORE

USE **TOOLS** TO HELP – FIDDLER, ZAP, BURP, BUG MAGNET

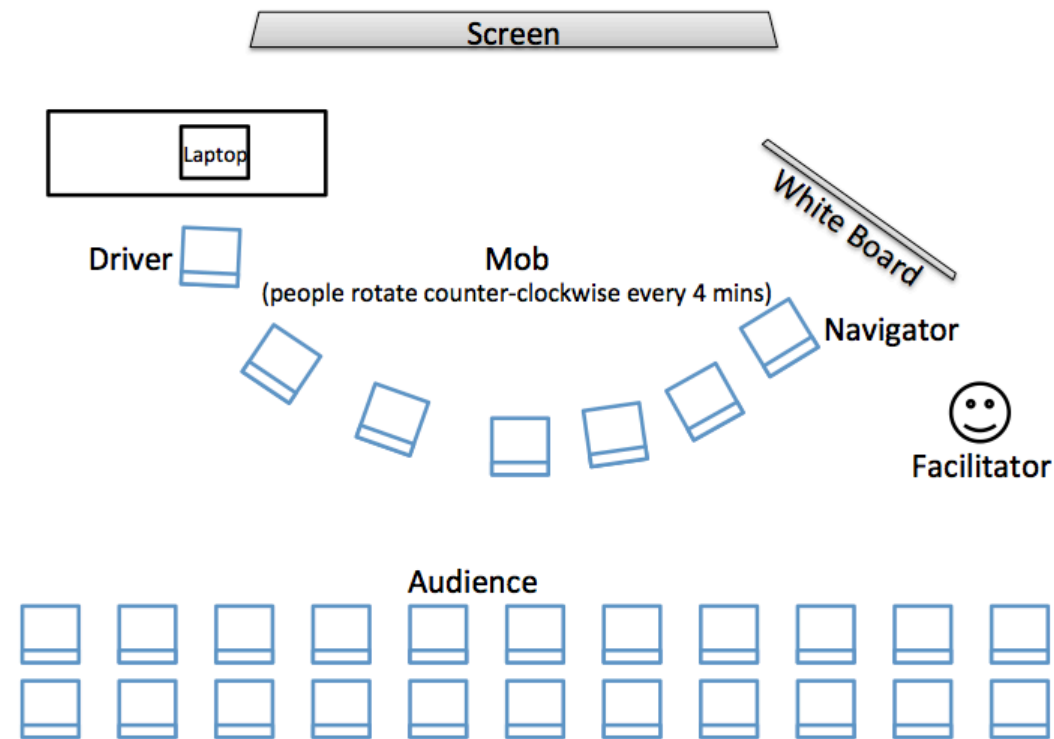
HAVE **FUN!**




MOB TESTING! WHAT IS IT?

RULES:

- NO **THINKING** AT THE KEYBOARD
- YES, **AND**...
- KINDNESS, CONSIDERATION AND RESPECT



VULNERABILITY: PASSWORD IN THE COOKIES

1. Register a user
 2. Locate the encrypted password
 3. Decrypt the password
 4. Use the decrypted password to login as the user
- 

HOW MANY TIMES CAN YOU VOTE?

Once?

Are you sure?

How can we exploit voting?

GET ADMIN ACCESS

Find a way to get Admin Access – look at cookies, look at the web traffic

What can an admin do?

RETROSPECTIVE
