
# What's wrong with penetration testing. By a penetration testing company.

OWASP

The Open Web Application Security Project

# About Me

OWASP
The Open Web Application Security Project

- Matthew Whitcombe
- Background in tech marketing and consulting
- With MWR since 2012

MWR
an F-Secure company

OWASP
The Open Web Application Security Project

Pen testing means something very specific to those buying & supplying it…

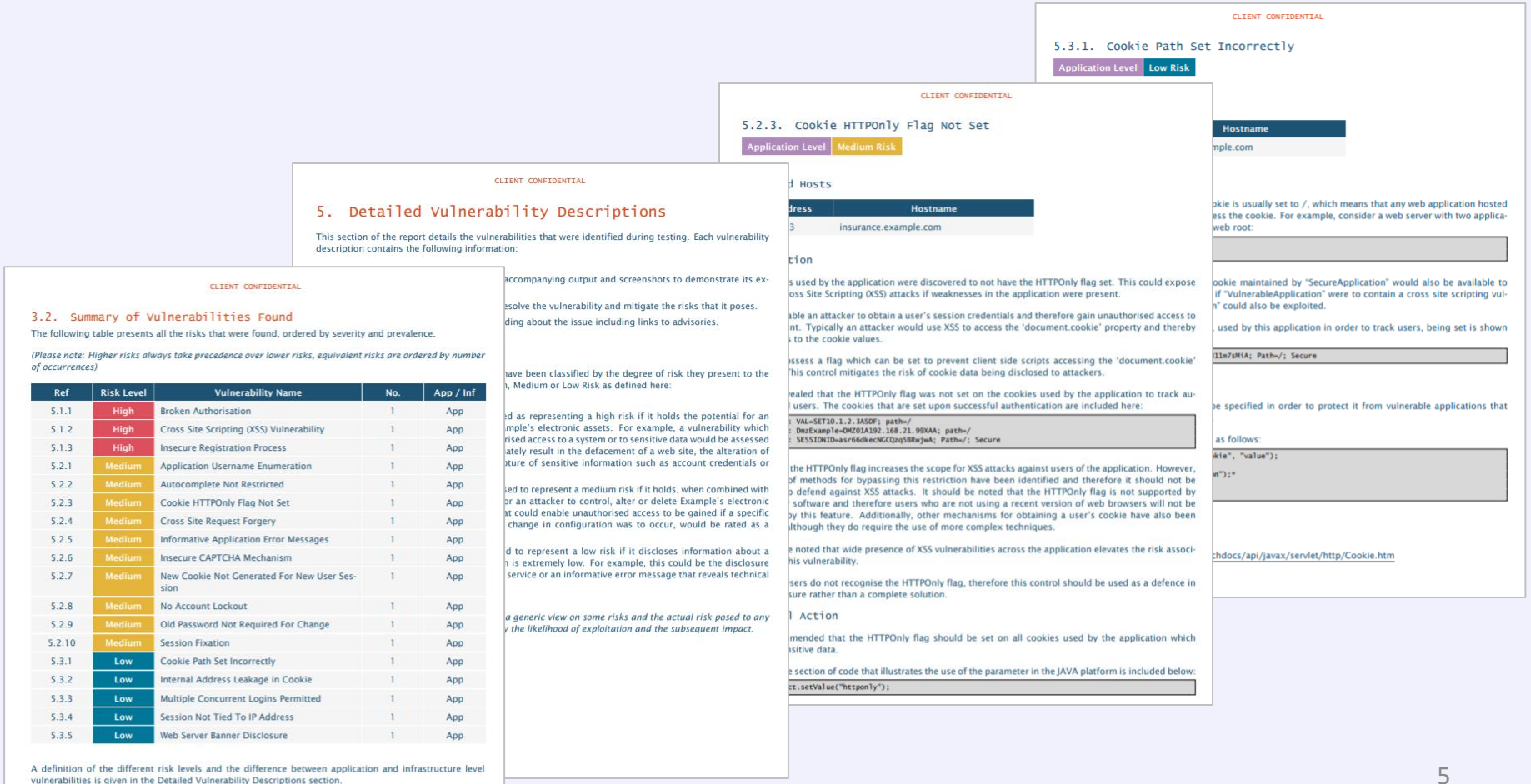
- *Give a piece of technology a once-over looking for vulnerabilities; report on these and on remediations*

What's wrong with that? 🤔

- *Give a piece of technology a once-over looking for vulnerabilities, report on these and on remediations*

OWASP
The Open Web Application Security Project

# A typical pen test report



CLIENT CONFIDENTIAL

## 3.2. Summary of Vulnerabilities Found

The following table presents all the risks that were found, ordered by severity and prevalence.

*(Please note: Higher risks always take precedence over lower risks, equivalent risks are ordered by number of occurrences)*

| Ref | Risk Level | Vulnerability Name | No. | App / Inf |
|---|---|---|---|---|
| 5.1.1 | High | Broken Authorisation | 1 | App |
| 5.1.2 | High | Cross Site Scripting (XSS) Vulnerability | 1 | App |
| 5.1.3 | High | Insecure Registration Process | 1 | App |
| 5.2.1 | Medium | Application Username Enumeration | 1 | App |
| 5.2.2 | Medium | Autocomplete Not Restricted | 1 | App |
| 5.2.3 | Medium | Cookie HTTPOnly Flag Not Set | 1 | App |
| 5.2.4 | Medium | Cross Site Request Forgery | 1 | App |
| 5.2.5 | Medium | Informative Application Error Messages | 1 | App |
| 5.2.6 | Medium | Insecure CAPTCHA Mechanism | 1 | App |
| 5.2.7 | Medium | New Cookie Not Generated For New User Session | 1 | App |
| 5.2.8 | Medium | No Account Lockout | 1 | App |
| 5.2.9 | Medium | Old Password Not Required For Change | 1 | App |
| 5.2.10 | Medium | Session Fixation | 1 | App |
| 5.3.1 | Low | Cookie Path Set Incorrectly | 1 | App |
| 5.3.2 | Low | Internal Address Leakage in Cookie | 1 | App |
| 5.3.3 | Low | Multiple Concurrent Logins Permitted | 1 | App |
| 5.3.4 | Low | Session Not Tied To IP Address | 1 | App |
| 5.3.5 | Low | Web Server Banner Disclosure | 1 | App |

A definition of the different risk levels and the difference between application and infrastructure level vulnerabilities is given in the Detailed Vulnerability Descriptions section.

CLIENT CONFIDENTIAL

## 5. Detailed Vulnerability Descriptions

This section of the report details the vulnerabilities that were identified during testing. Each vulnerability description contains the following information:

CLIENT CONFIDENTIAL

## 5.2.3. Cookie HTTPOnly Flag Not Set

Application Level | Medium Risk

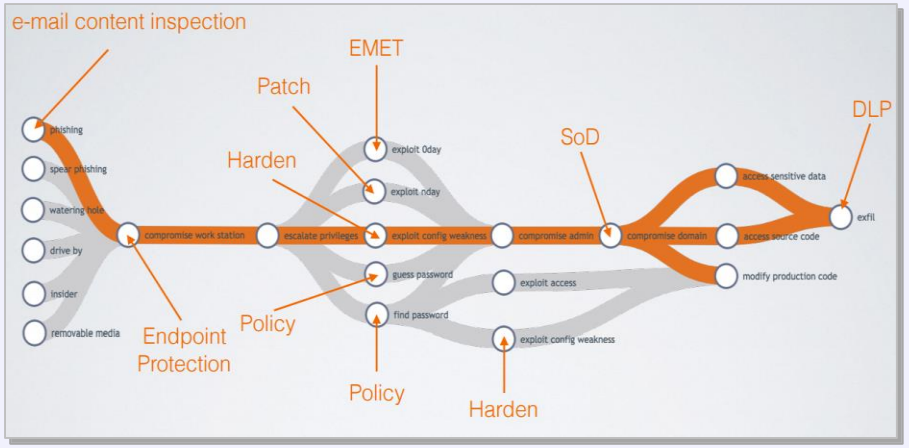
CLIENT CONFIDENTIAL

## 5.3.1. Cookie Path Set Incorrectly

Application Level | Low Risk

# Attack Path Mapping

- Collaborative, 'white-box'
- Starts with *assets* that matter most (usually a bounded scope)
- Considers *all* attack paths real attackers would use



OWASP
The Open Web Application Security Project

# Attack Path Mapping

- Collaborative, 'white-box'
- Starts with *assets* that matter most (usually a bounded scope)
- Considers *all* attack paths
  real attackers would use
- Then technical testing to validate
- Then recommend how to close *unintentional* paths, or strengthen controls on *intentional* paths

# Attack Path Mapping

## +ve

- Reports talk to business managers
- *Prioritises* remediation investments
- Recommendations are pragmatic, with buy-in from client's SMEs
- Low-ish cost

## –ve

- Needs time input from client's SMEs
- It's different

# Red teaming

- Open-scope, simulated attack to find if you can be compromised, and understand how

# Red teaming

## +ve

- Not confined to a piece of technology
- The ultimate acid test of prevention, detection & response
- Exciting! 

## –ve

- Expensive
- Doesn't answer 'If'. (You can. Get over it.)
- Illuminates a tiny percentage of 'How'
- Horribly stressful
- Can lose sight of *helping improve* detection & response in realistic scenarios

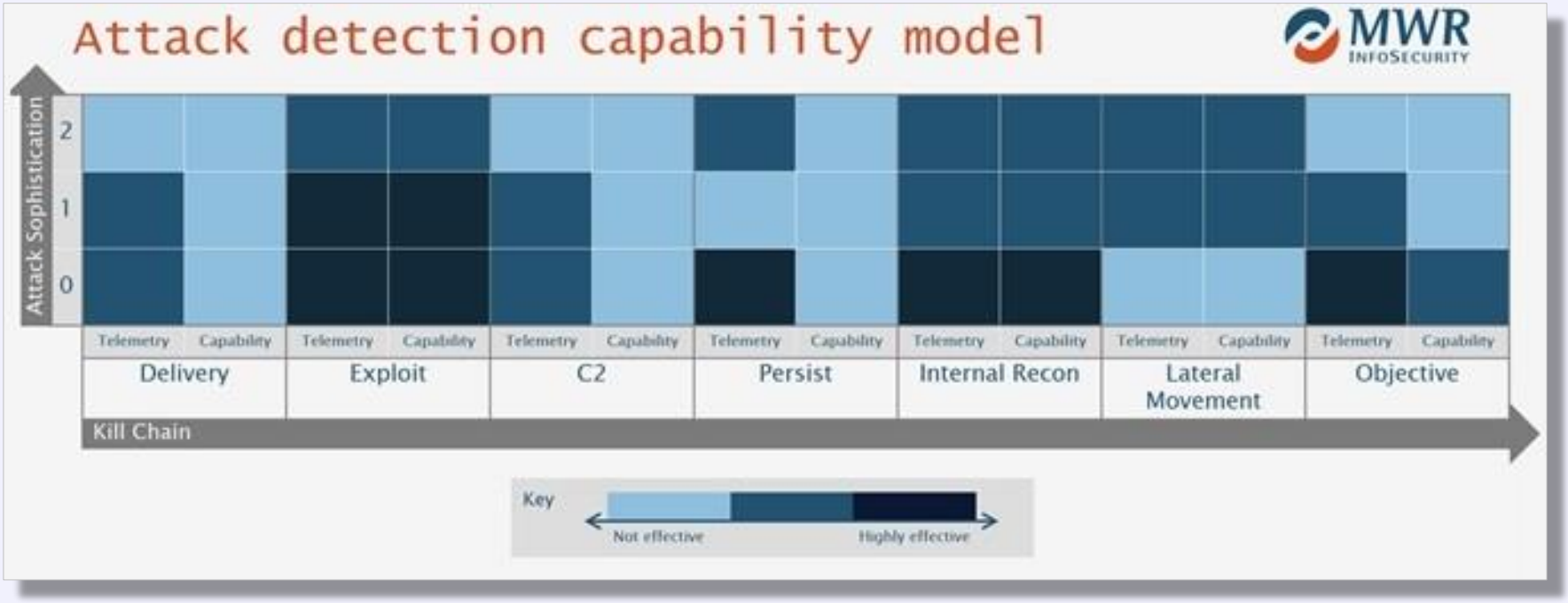
It's like playing squash…

OWASP
The Open Web Application Security Project

# Purple teaming

- Collaborative, not adversarial
- Knowledge sharing between Red (attack) and Blue (defence) teams
- Example: Reds sit with Blues and jointly throw hundreds of different test cases (attacker techniques & tools) at the SOC's *detection* capabilities

# The results look like this…



# Purple teaming

## +ve

- Avoids stresses of stealthy red teaming – can *aid* SOC morale
- Unlike red teaming, maximises learnings across a huge scope of attacker actions
- Eases comparisons – over time, and between organisations

## –ve

- Needs acid test of occasional full-contact red team to satisfy the sceptical

It's like cross-training…

OWASP
The Open Web Application Security Project

# Threat hunting

- Continuous, analyst-driven, hypothesis-based, proactive search for the traces that advanced attackers would leave behind

- Live hand-to-hand response to unfolding attacks

OWASP
The Open Web Application Security Project

# Threat hunting

## +ve

- The attacker only has to make one mistake
- Isn't entirely dependent on tools & technology
- 'Incident Response' != mopping up the damage

## –ve

- Not cheap
- Skills are scarce
- Can get diverted into a tools-fest if you're not careful

OWASP
The Open Web Application Security Project

# Continuous Assurance

- An innovative way of thinking we believe is long overdue in the industry
- Ongoing, daily examination of the IT estate to pinpoint emerging problems & recommend immediate fixes
- Most work so far is in external-facing technologies, and SDLC

# Continuous Assurance

## +ve

- Removes risks of point-in-time testing
- Alerts to changes that really matter, and what to do about them

## –ve

- New and embryonic
- Most work is pilot or early stage
- Can get diverted into a tools-fest if you're not careful

OWASP
The Open Web Application Security Project

# Questions?