Web Security and the OWASP Top 10: The Big Picture

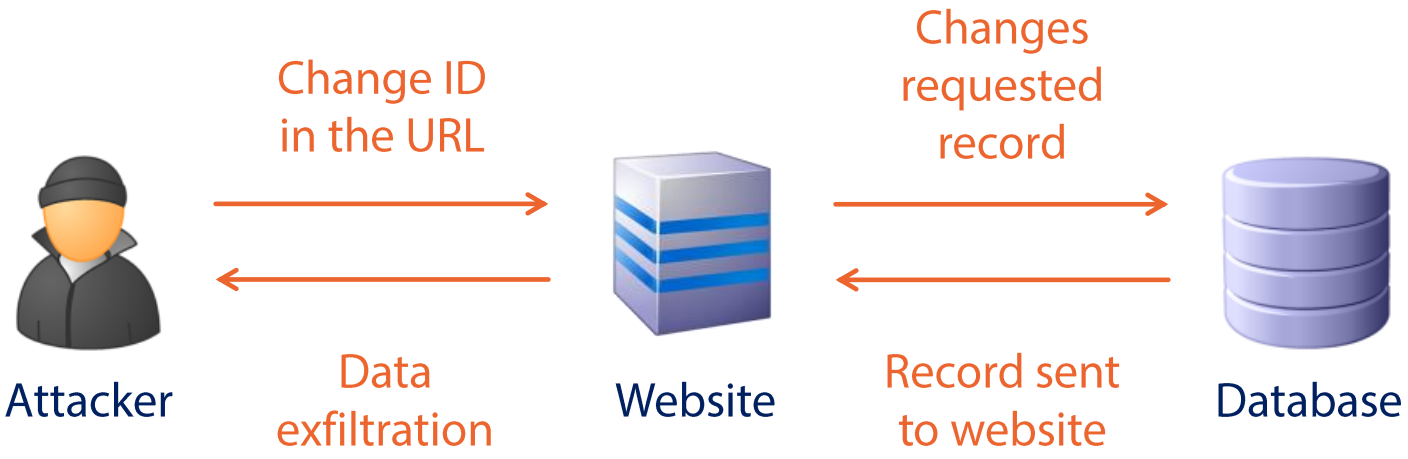
Insecure Direct Object References

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Insecure Direct Object References Overview

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



Understanding Direct Object References

http://mybank.com/Balance?AccountId=293843

http://mybank.com/Balance?AccountId=498274

http://mybank.com/Balance?AccountId=984353

Untrusted

Common Defences Against Direct References

Implement access controls

- Be explicit about who can access resources
- *Expect* the rules to be tested

Use indirect maps

- Don't expose internal keys externally
- Map them to temporary ones

Avoid predictable keys

- Incrementing integers are enumerable
- Natural keys are discoverable

Direct Object References in the Wild – Citigroup Hack

Citigroup hack exploited easy-to-detect web flaw

Brute force attack exposes 200,000 accounts

Hackers who stole bank account details for 200,000 Citigroup customers infiltrated the company's system by exploiting a garden-variety security hole in the company's website for credit card users, according to a report citing an unnamed security investigator.

The New York Times reported that the technique allowed the hackers to leapfrog from account to account on the Citi website by changing the numbers in the URLs that appeared after customers had entered valid usernames and passwords. The hackers wrote a script that automatically repeated the exercise tens of thousands of times, the *NYT* said in an article published Monday.

"Think of it as a mansion with a high-tech security system – that the front door wasn't locked tight," reporters Nelson D. Schwartz and Eric Dash wrote.

The underlying vulnerability, known as an insecure direct object reference, is so common that it's included in the Top 10 Risks list compiled by the Open Web Application Security Project. It results when developers expose direct references to confidential account numbers instead of using substitute characters to ensure the account numbers are kept private.