Web Security and the OWASP Top 10: The Big Picture

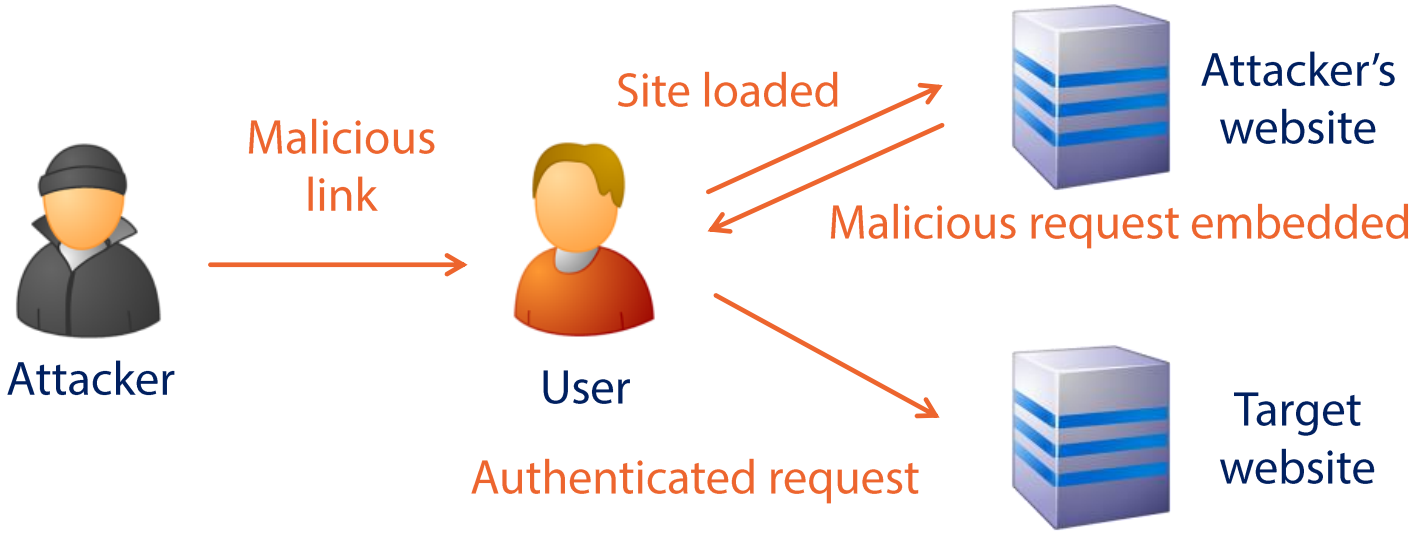
Cross-Site Request Forgery (CSRF)

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

CSRF Overview

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



Understanding CSRF

User

Authenticated request to transfer money online

Website

```
HTTP POST https://mybank.com/transfer

Auth-cookie: 87e090ace8…

TargetAccNum: 8781648823
Amount: 1000000.00
```

Attacker forges request

Common Defences Against CSRF

Employ anti-forgery tokens

- CSRF is exploited by predictable patterns
- Tokens add randomness to the request

Validate the referrer

- Valid requests don't originate externally
- The referrer is in each request header

Other defences

- Native browser defences
- Fraud detection patterns

CSRF in the Wild – Brazilian Modems

How millions of DSL modems were hacked in Brazil, to pay for Rio prostitutes

by Graham Cluley on October 1, 2012 | 15 Comments

FILED UNDER: Featured, Malware, Phishing, Vulnerability

So, you think you're doing a pretty good job in terms of computer security on your home PC? You've kept your computer fully patched against the latest vulnerabilities? You've ensured that your PC is running the latest-and-greatest anti-virus updates?

Good for you.

Now, how about your router?

My suspicion is that the typical computer user doesn't give a second thought about whether their router could be harbouring a security threat, imagining that the devices don't need to be treated with suspicion.

But if you think that, you're quite wrong.

Fabio Assolini, a researcher for Kaspersky Labs, gave a fascinating presentation at the Virus Bulletin conference in Dallas last week, describing how more than 4.5 million home DSL routers in Brazil were found to have been silently hacked by cybercriminals last year.