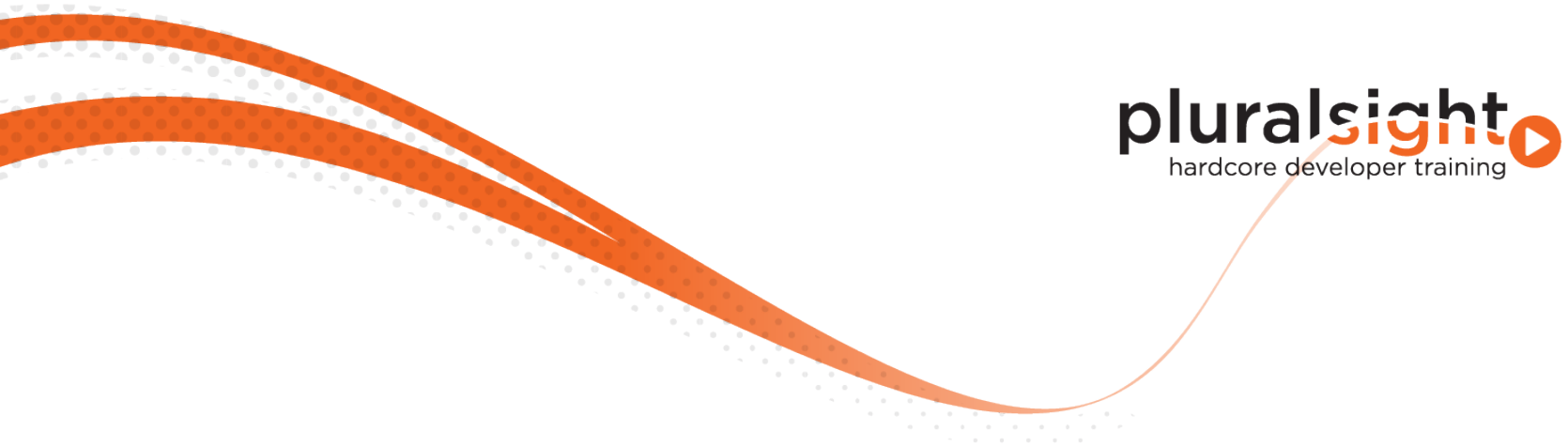
# Unvalidated Redirects and Forwards

Troy Hunt
troyhunt.com



# Outline

- How OWASP views the risk
- Performing an attack against a vulnerable application
- The value of unvalidated redirects to attackers
- Using whitelists and referrer checking to thwart malicious use
- Other general issues with the risk

# OWASP overview and risk rating

| Threat Agents |
| --- |
| — |
| Consider anyone who can trick your users into submitting a request to your website. Any website or other HTML feed that your users use could do this. |

# Understanding the value of unvalidated redirects to attackers

- Unvalidated redirects are useful to attackers as they abuse the trust the victim has in the target site
- A URL such as this may arouse suspicions:

```
http://evilsite.com/malware.exe
```

- But a URL such as this will almost certainly be trusted:

```
http://trustedsite.com/redirect?url=
```

# Delivering “loaded” URLs

- **Attackers may distribute the malicious payload in the redirect URL by all the common means:**
  - Email phishing scams
  - Social media
  - Compromised legitimate sites
- **Because the domain of the address is trusted, detection of the risk through automated tools such as spam filters is harder**
- **Tools such as Twitter also often only show the first part of the address (domain and part of the path) before users click it**
- **The redirect payload may be obfuscated by URL encoding *every* character**
  - This makes it near impossible to visually identify that the embedded URL is malicious

# Other issues with unvalidated redirects

- **This is often viewed as a "light" risk**
  - It's not  vulnerability in the site itself…
  - …but it *does* allow the site to be used as a launch pad for an attack
- **Google has elected not to pay bug bounties for the risk:**

> *"While we prefer to keep their numbers in check, we hold that the usability and security benefits of a small number of well-implemented and carefully monitored URL redirectors tend to outweigh the true risks."*

# The risk is about reputation

- **Unvalidated redirects don't actually expose data on the site or do any direct damage to it**
- **However, for victims of an attack using unvalidated redirects, the site in question appears to be the malicious one**
  - They trusted the domain and what in their view was content on the site
- **This is a reputation risk – it *appears* as though the site is compromised**

# Summary

- **Unvalidated redirects pose value to attackers as they provide a legitimate point from which to launch an attack**
  - Trustworthy domains are preferred
- **There is a valid use case for redirects, but usually only for forwarding a user to *trusted* addressed**
  - We're back to whitelists again
- **Referrer checking can mitigate the risk, but not entirely eradicate it**
- **It's not always viewed as a major risk, indeed it's at the very end of the Top 10!**
  - Plus Google won't pay you any money for reporting it as a bug
  - But consider the risk to reputation