Video Responses will be based around the summary of the OWASP Top 10 which are the most common/worst web vulnerabilities out there.

1. Broken Access Control
2. Cryptographic Failures

Find examples of these two in real software, not CTFs.

Look in:

* CVE Database
* Blackhat talks
* Whitepapers
* Academic Papers

For project 2 way may have to implement a challenge using these exploits

**JavaScript Continued:**

Quality of Maintenance Score given by researchers to give an idea of how likely a website would be to get breached.

Class Ideas for ways to create a quality of maintenance score:

* Frequency of updates
* State/Lifetime of Support
* Company Reputation
* VirusTotal Check

Command & Control servers are what give BotNets their instructions

Researchers Quality of Maintenance:

* Availably, expired?
* Cookie Attributes
* SSL/TLS Implementation
* Webserver version (Information contained in the HTTP Header for server response)

**JavaScript 3rd Party Script Attacks:**

1. Cross-User / Network Scripting

* Src: 127.0.0.1 (Local Host IP)

1. Expired Domains

* 47/10,000 domains were expired and purchased by the researchers
* In 15 days they say 86k requests

1. Typo Squating

* When attackers buy a domain that is one letter off on the original hoping for people to visit the website by mistake.
* Researches Typo Squatted on googlesyndicatio.com because that’s the website that is included in the google ads javascript
* Over 15 days they say 165k requests to that URL, from over 2,000 different domains

**Solutions To Protect Against Attacks:**

* Build in protection to the browser
* Principle of Last Privilege
* Sandboxing

**Challenge 1:**

Coming up with the policy itself to decide what a JavaScript script can access

**Challenge 2:**

How to check against which scripts have been updated

**DNS**

Serves as a defacto Root-of-Trust for domain names across the internet

**Residual Trust:**

When someone buys a domain that was once well regarded

**2016 Oakland Paper by Lever “28 Registration later….Measuring Abuse of Residual Trust”**