Hacking THAT

Real-World Penetration Testing


THAT
CONFERENCE

Art Kay

Engineering Lead - Web
IronNet Cybersecurity

Chicago-land

www.akawebdesign.com

THANK YOU, THAT CONFERENCE SPONSORS!

CUNA MUTUAL GROUP

Northwestern Mutual

Microsoft

twilio

ZYMO INTERACTIVE

spr

NVISIA

Created by ThoughtWorks go

GrapeCity

Particle

TASC

New Relic

shopify

THAT Kay Family

- 6th of 7 years
- 5th year as speaker
- 2nd year re: “The Cyber”


All of this computer hacking is making
me thirsty. I think I'll order a 'tab'.

What is a penetration test?

Agenda

- Methodology
- Information Gathering
- Vulnerabilities
- Exploitation
- Resources

Stuff I'm Going to Skip

http://www.pentest-standard.org

- Planning and Scoping
- Reporting
- Legal complications

Take-Aways

“The Cyber”

1. How hackers attack a web application

2. Things ThatConference is doing well…

   ...and not so well.

3. You should actively think about security!

---

0. Methodology

Before you start...

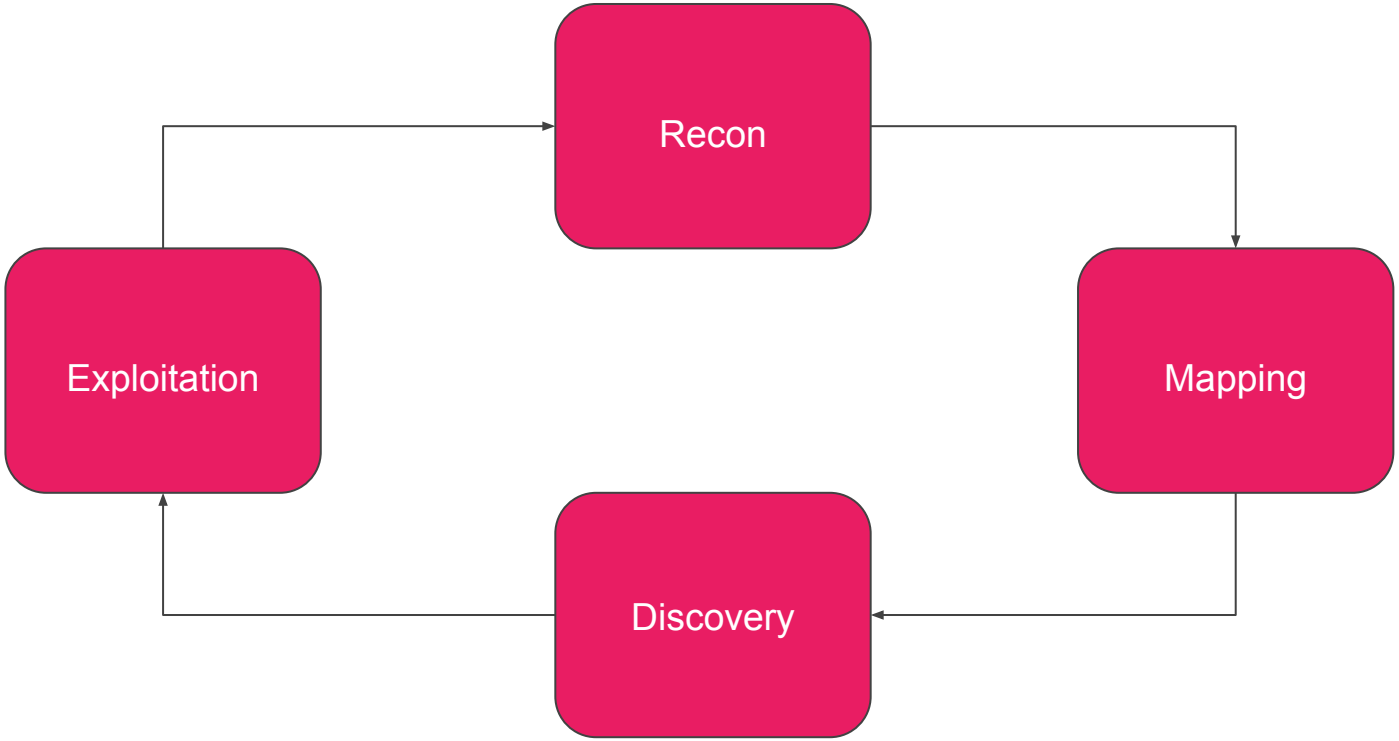
Get ***expressed written permission*** from:

- Owner of site/service
- Owner of server

The FBI will not be amused.

Ignorance is not an excuse.

Don’t do anything stupid.

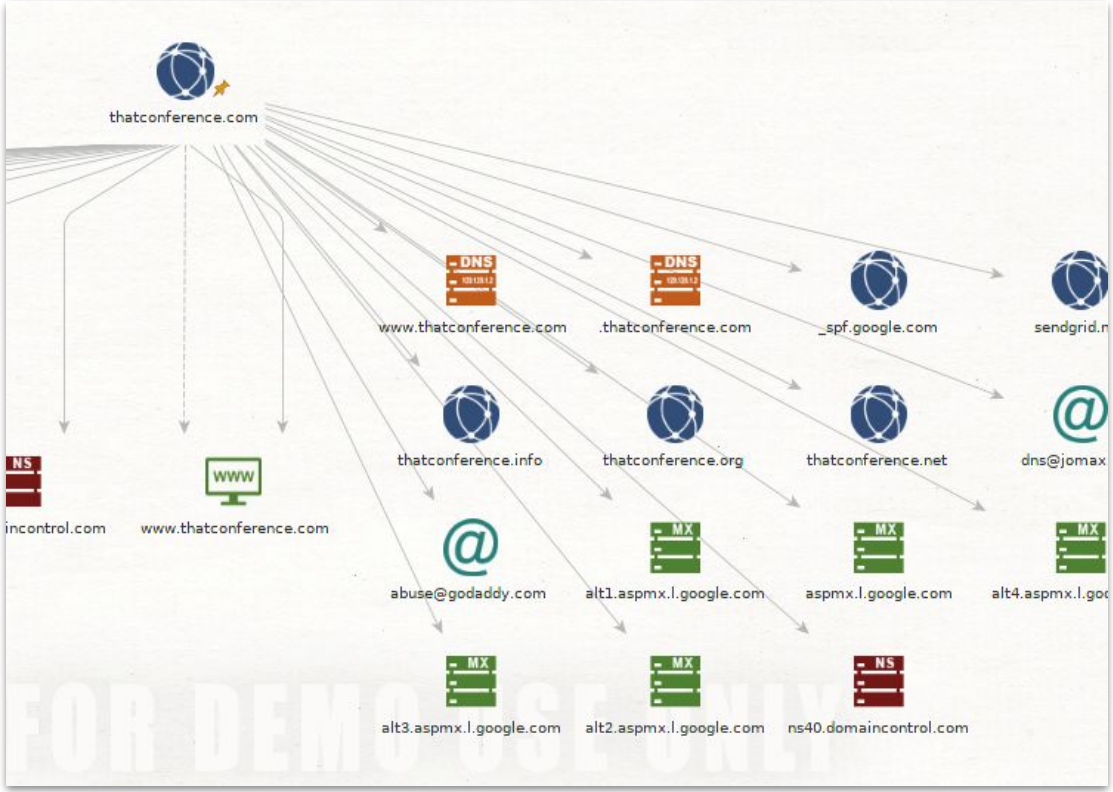


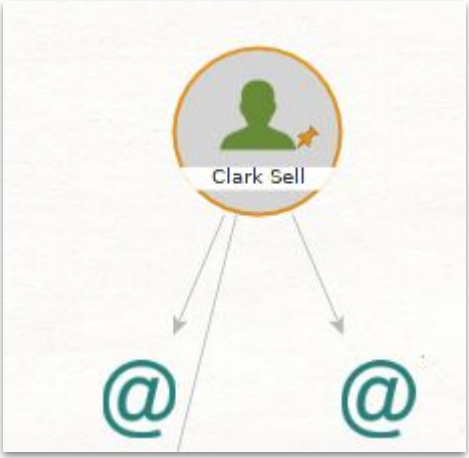
Methodology

Target: ThatConference.com

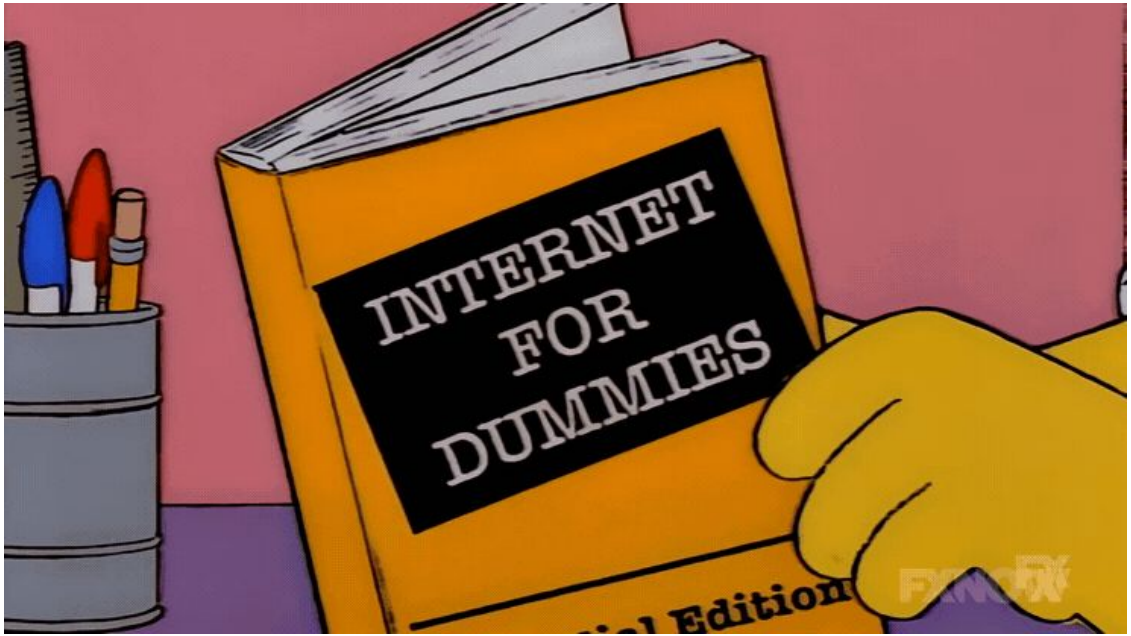
1. Recon

Mental Map


thatconference.com
DNS
www.thatconference.com
DNS
.thatconference.com
_spf.google.com
sendgrid.n
thatconference.info
thatconference.org
thatconference.net
dns@jomax
NS
incontrol.com
www
www.thatconference.com
abuse@godaddy.com
MX
alt1.aspmx.l.google.com
MX
aspmx.l.google.com
MX
alt4.aspmx.l.goo
MX
alt3.aspmx.l.google.com
MX
alt2.aspmx.l.google.com
NS
ns40.domaincontrol.com
FOR DEMO USE ONLY


Clark Sell

Recon: Active vs Passive



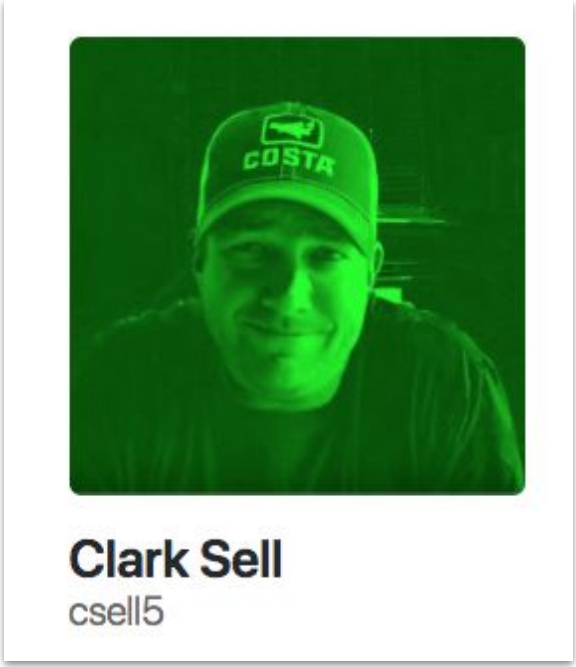
Active Vs Passive

Do you want your IP address exposed?

If you can see them, they can see you.

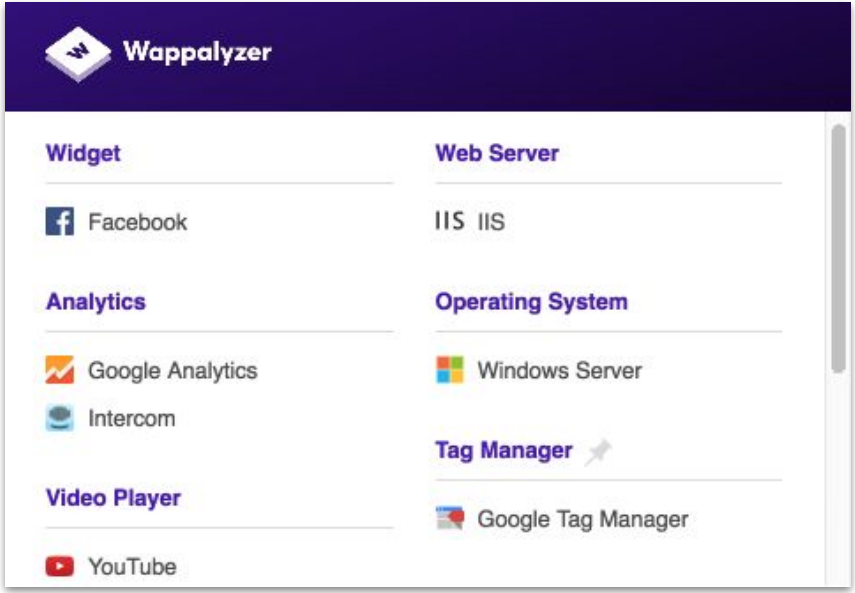
Passive Recon

- Names and Emails
- Registered Domains
- WHOIS information
- Social Media



Active Recon

- Subdomains
- Technologies involved
- Known Vulnerabilities
- Word lists
- Known users



Tools

RECON

- dnsenum
- dnsmap
- nmap

- Social Media

- browser DevTools
- browser extensions

- ...so many more...

What did we learn?

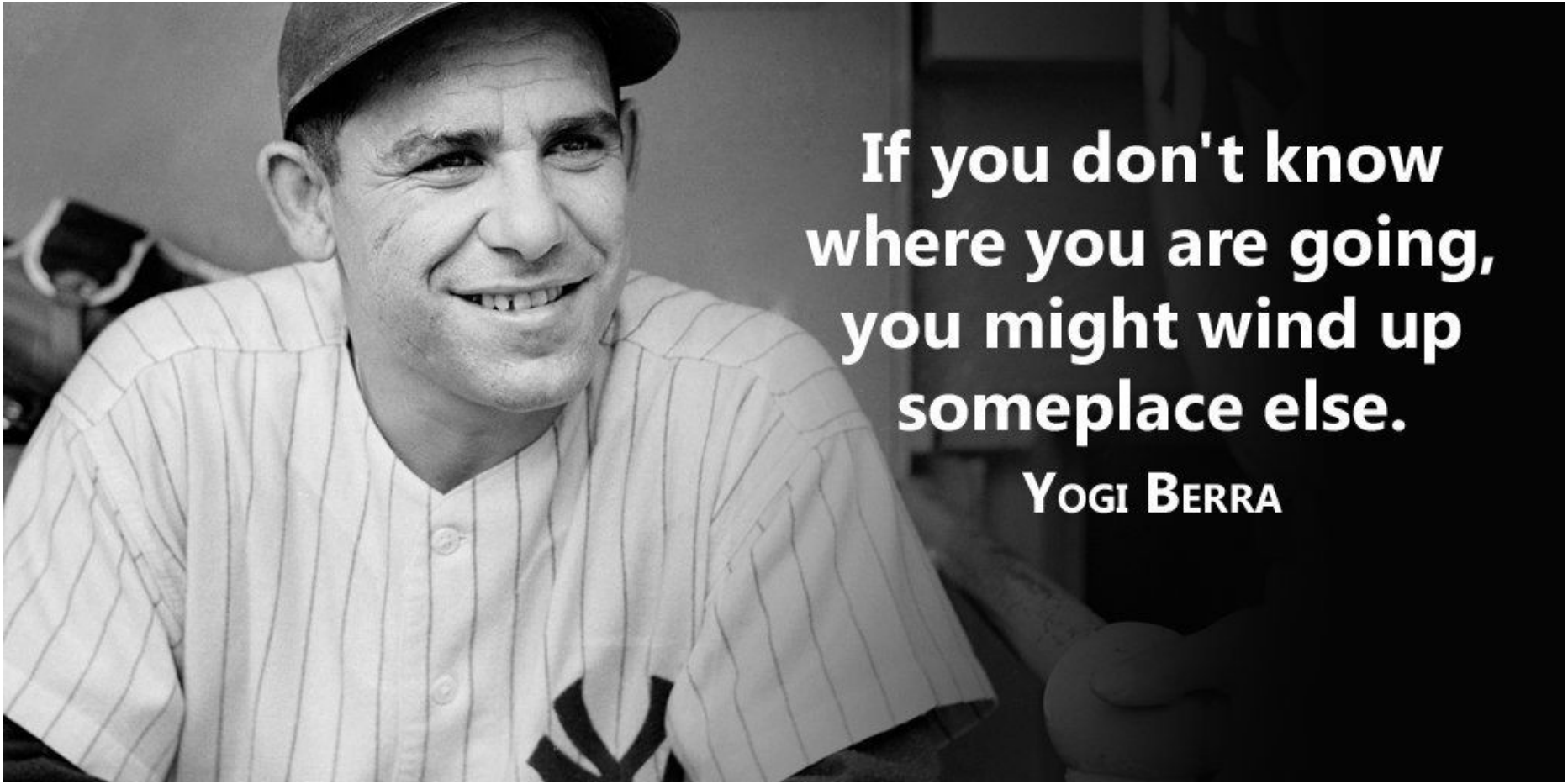
- A LOT about DNS and network topology

- Pretty good idea who the main developers are

- ASP.NET vX.X.XYZ
- ASP.NET MVC vX.X
- IIS 10.0
- AngularJS v1.5.8

---

2. Mapping


If you don't know where you are going, you might wind up someplace else.
Yogi Berra

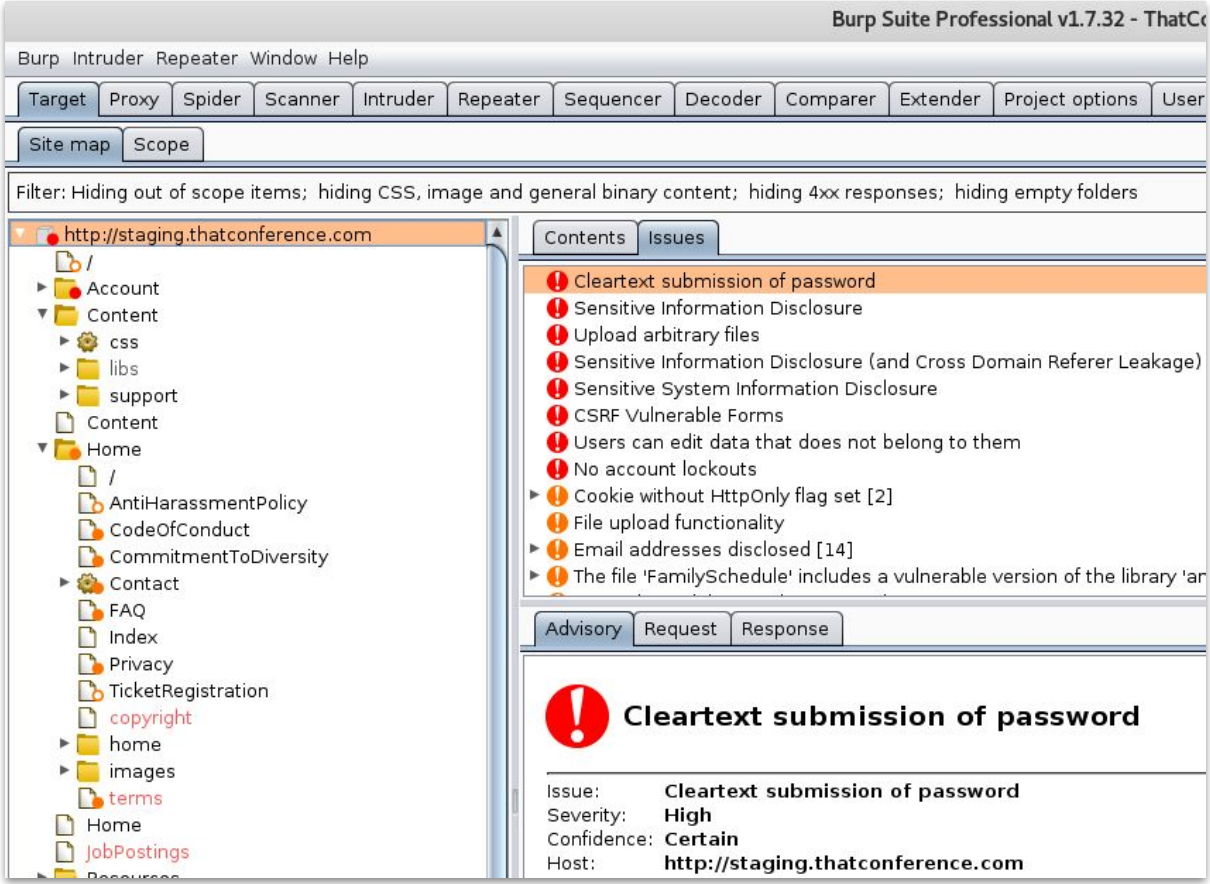
Tools

MAPPING

- Burp
- Firefox / FoxyProxy

Mapping

- Files, folders, APIs
- Spiders
- Authenticated?



What did we learn?

- JavaScript API requests
- HTTP Requests/Responses
- HTTP parameters
- Cookies & Tokens
- The overall purpose of the application

---

3. Discovery

Questions: Authentication

- How do you login, logout, change passwords?
  - Different user types? ⚠ Maybe
- Does the app reveal if usernames are valid? ⚠ Maybe
- Does the app attempt to prevent automated attacks? ⊘No!
  - CAPTCHA
  - Account lockouts
- Does the app provide a mechanism for account recovery? ⚠ Yes

Questions: Session Management

- What does the app use for session tracking?
- Are the session's contents viewable? ✓No!
- Is the session deleted upon logout? ✓Yes!
- Are the cookies protected with flags? ⊘No!
  - secure, httpOnly, sameSite
- Do sessions expire? ⚠ Maybe

Other Questions

- Do all XHR go through a single endpoint? ✓Yes
- What user inputs get reflected to the user?
- What user inputs are used in queries?
- Are any user inputs used in system commands? ✓No!
- Do any user inputs determine destination or redirect? ⚠ Yes
- Can users upload files to the server? ⚠ Yes
- Do sequential process flows exist? ✓No!

What did we learn?

- Probably different user roles
- We could probably brute-force login attempts
- Sessions look pretty solid, but maybe CSRF vulnerable
- User profile looks ripe for abuse
- File uploads *ERMAGHERD*
- URL redirects exist -- we should explore those

4. Exploitation

2017 OWASP

TOP 10

APPLICATION SECURITY RISKS

A1 INJECTION

A2 BROKEN AUTHENTICATION

A3 SENSITIVE DATA EXPOSURE

A4 XML EXTERNAL ENTITIES (XXE)

A5 BROKEN ACCESS CONTROL

A6 SECURITY MISCONFIGURATION

A7 CROSS-SITE SCRIPTING (XSS)

A8 INSECURE DESERIALIZATION

A9 USING COMPONENTS WITH KNOWN VULNERABILITIES

A10 INSUFFICIENT LOGGING & MONITORING

21 Vulnerabilities*

*Not an indication of bad design/code.

*Most already patched.

*Not all were exploitable.

*Your application probably has that many too. Or more.

Tools

EXPLOITATION

- Burp

Server Information Exposed in HTTP Headers

- X-Powered-By
- X-AspNet-Version
- X-AspNetMvc-Version
- Server

An attacker will immediately use this information to research vulnerabilities against your technology stack.

Don’t give this away for free!

SQL Injection / XSS

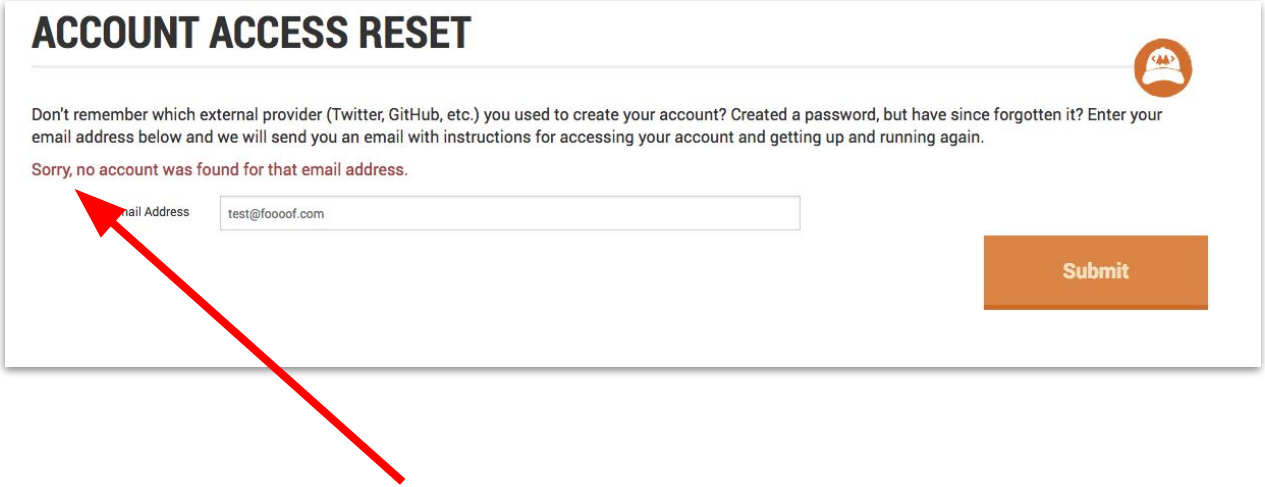
SQL Injection allows an attacker to read or modify information stored in your database.

Cross-Site Scripting (XSS) attacks allow attackers to access cookies, session data, and other sensitive information. Can be “stored” or “reflected”.

Sensitive Data Disclosure

The account recovery form will respond telling a user whether-or-not a given email address has an account.

This obviously helps an attacker learn which email addresses are valid -- narrowing down a list of accounts to try breaking into.



No Account Lockouts

Malicious users can brute-force login attempts with impunity.

Once a known username is found, an attacker can send unlimited login attempts to guess passwords.

Insecure Direct Object Reference

- a.k.a Art pwns all sessions on THAT website

- Apologies to Aaron Douglas!

When an application provides direct access to objects based on user-supplied input.

Attackers can bypass authorization and access resources in the system directly, for example database records or files

5. Resources

Books

- **The Web Application Hacker’s Handbook**
  - Stuttard / Pinto
- **Mastering Kali Linux for Web Penetration Testing**
  - Michael McPhee

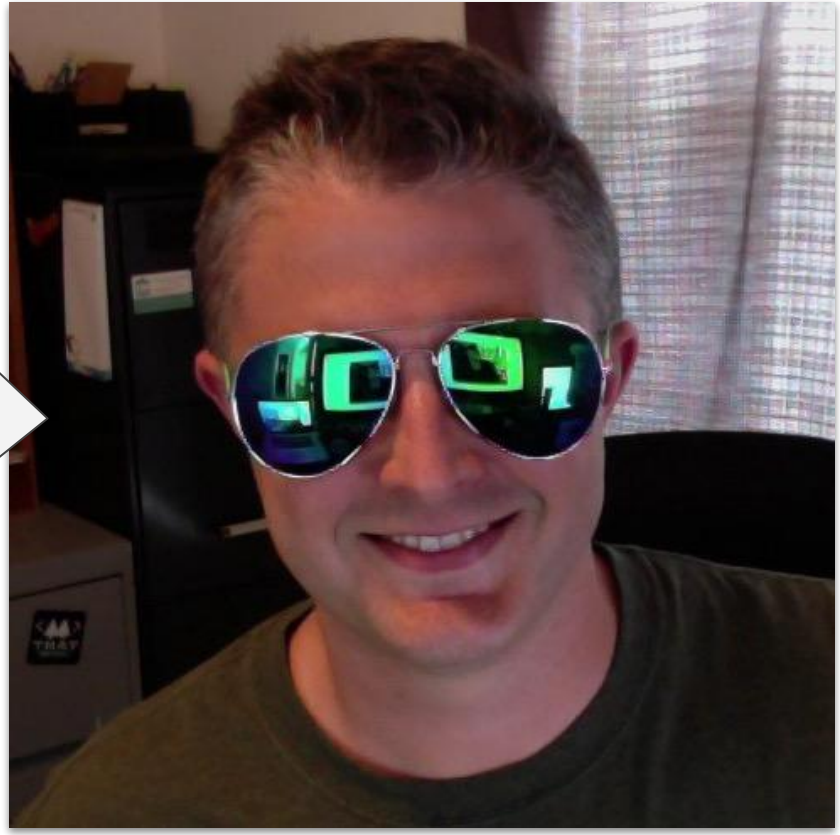
WWW

- Pentest-Standard.org
- OWASP.org

- ***akaWebDesign.com (blog)***

Thank You!

Questions?




THAT
CONFERENCE
SEE YOU NEXT YEAR!
AUGUST 5 - 7, 2019