

Automating Security Defenses

The Application Strikes Back

whoami

- Nathaniel (Nat) Shere
- Cybersecurity Consultant
 - Penetration testing (“ethical hacking”)
 - Secure Web Development
- Security Engineer
- Hobbies: security, programming, board games

What I Will Cover

- Importance of proactive security
- Current strategies – Reactive vs. Proactive
- The Application Strikes Back

A Word of Caution

- Don't hack back!

Importance of Proactive Security



“An ounce of prevention is worth a pound of cure.”

— Benjamin Franklin

tags: preparation, prevention, proverb, wisdom

287

The average number of days to identify a data breach in 2020

Source: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>

80

The average time (days) to contain a breach in 2020

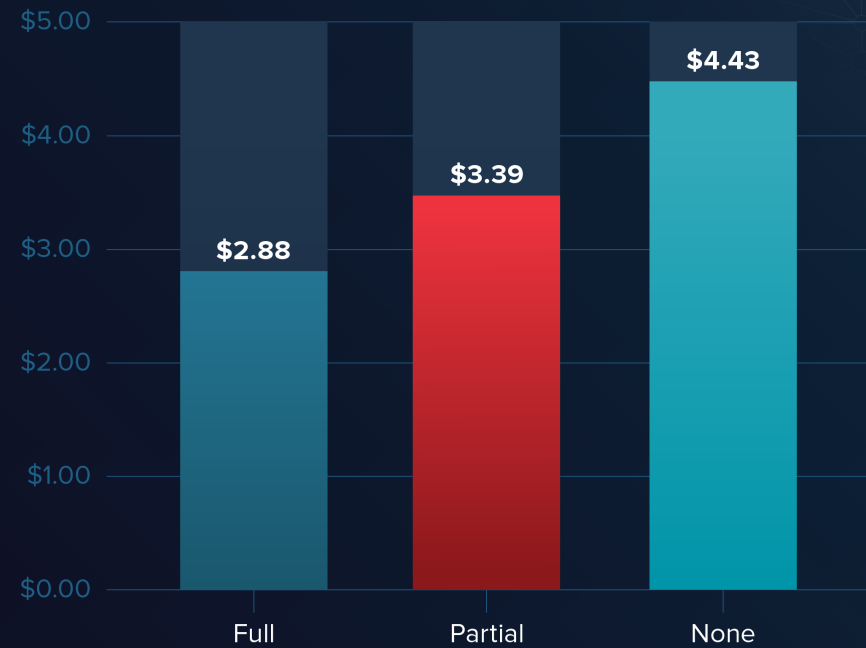
Source: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>

367

The average length (days) of a breach in 2020

Source: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>

Automation Decreases Cost of Data Breach



Average total cost (US\$ millions) based on security automation execution level
Source: IBM



Source: <https://www.varonis.com/blog/data-breach-response-times>

Security Strategies

- Reactive
- Proactive

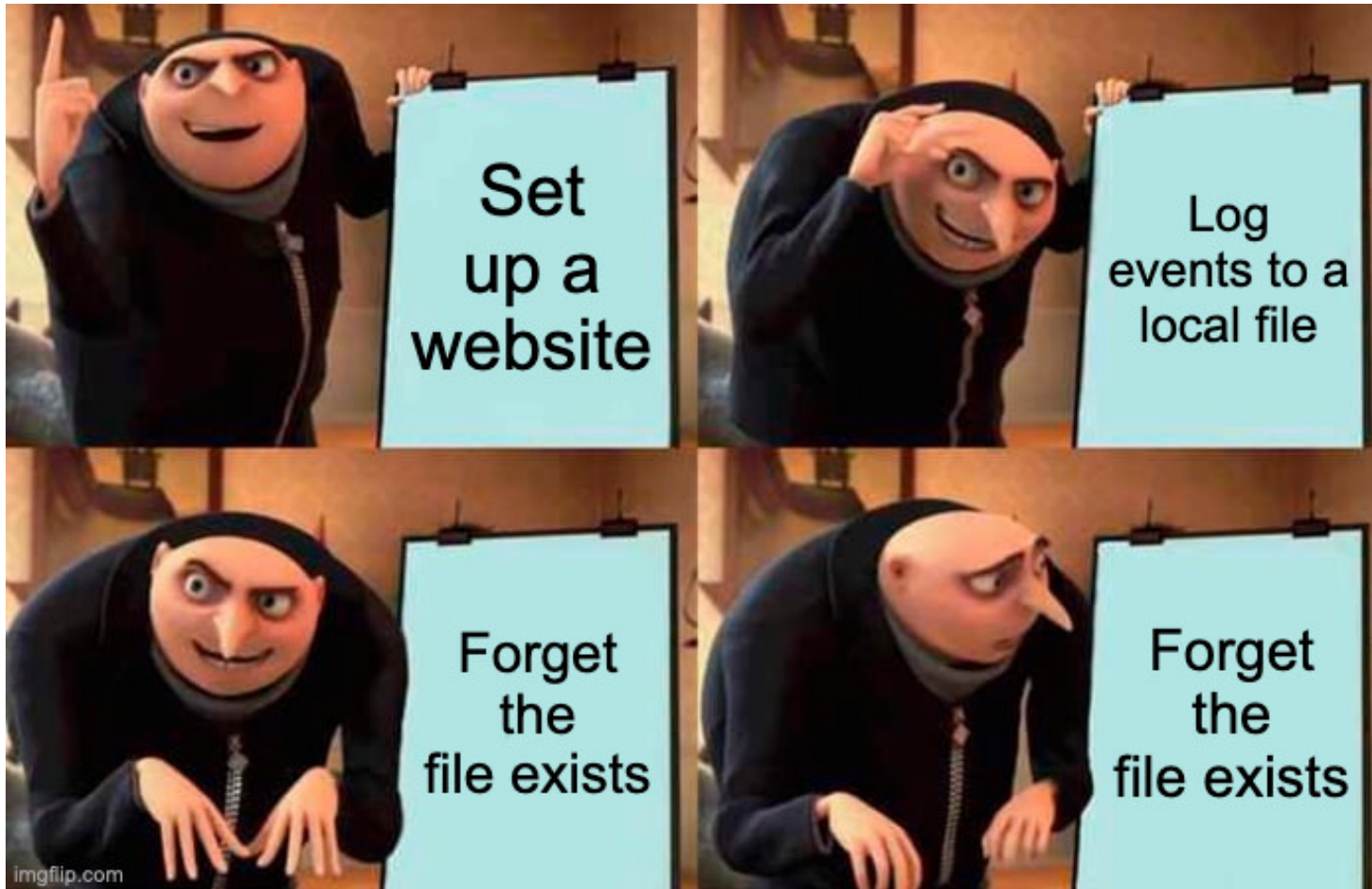
Security Strategy Goals

- *Reduce* time for security to detect attacker
- *Increase* time for attacker to find and exploit vulnerability

Reactive Strategies: No News is Good News

1. Set up a website
2. Pray you don't see your company name in the security news

Reactive Strategies: Checkbox Security



Reactive Strategies: Security Operations Center (SOC)

1. Implement logging
2. Collect logs in centralized place
3. Add rules and correlation logic to logs
4. Implement alerting based on triggers and thresholds
5. Identify stakeholders and asset owners
6. Create triage steps and playbooks for each alert
7. Add rules and correlation logic to alerts
8. Implement new tools and software
9. Configure the tools
10. Test the tools in your environment
11. Realize something isn't logging correctly
12. Realize stakeholders changed
13. Etc. etc. etc.

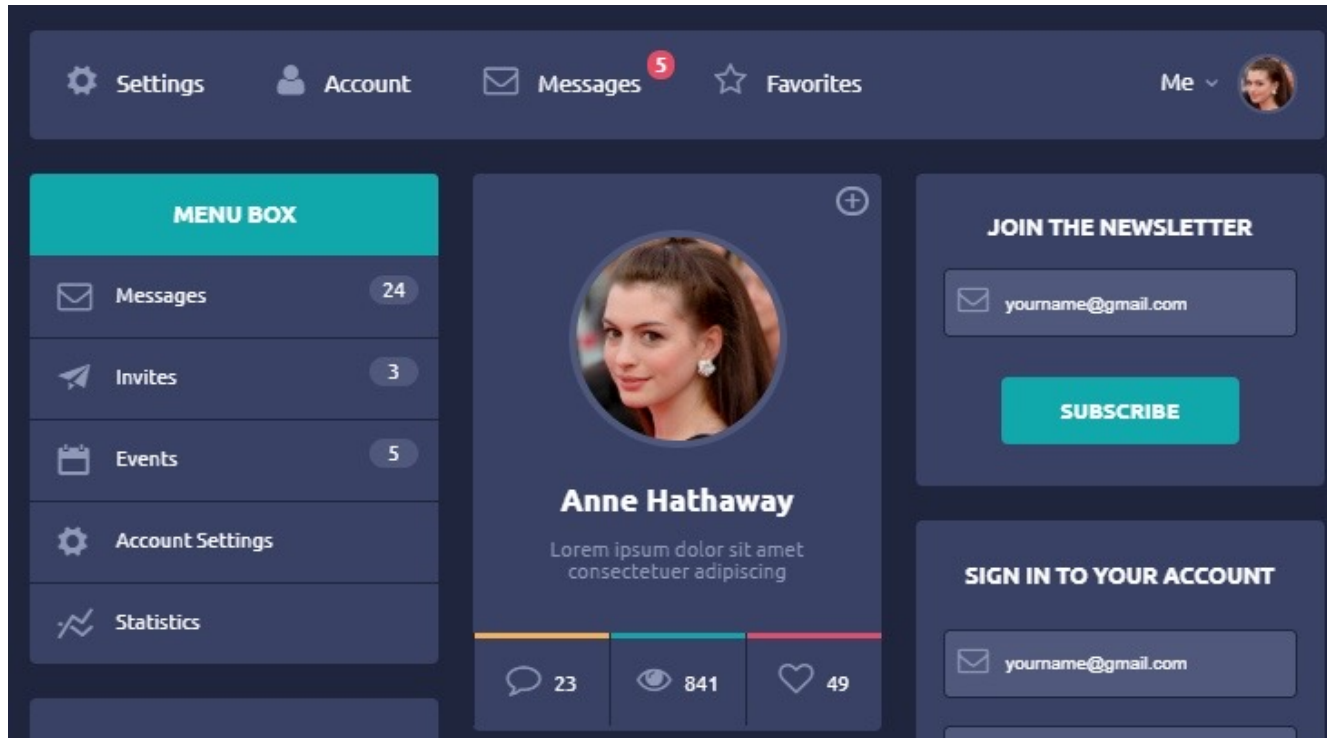
The Application Strikes Back



Hybrid Strategy: Alert from the Application

1. Identify a security risk in your application
2. Send an alert from the application if the risk is triggered
3. Block the offending user/source IP
 - Table of blocked sources
 - Automated request to WAF

Identify Security Risk: Data Enumeration



GET /users/**4**/profile

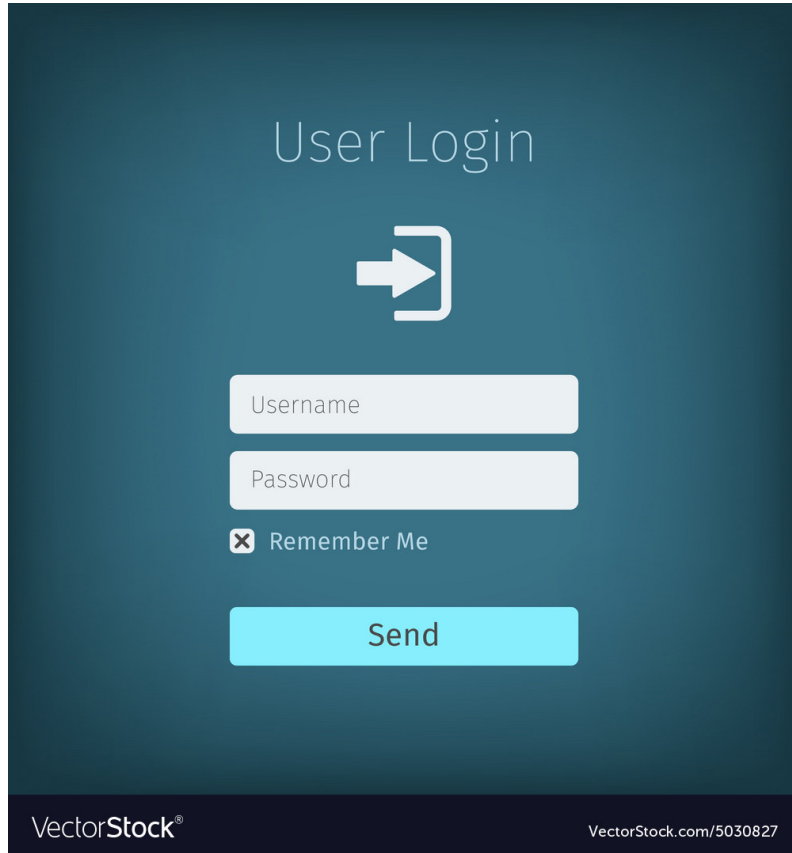
Identify Security Risk: Data Enumeration

GET /users/**4**/profile

GET /client/**75**/edit

GET /invoice/**1d68ea56-e458-4f0d-bf26-9fcc5dd31e6a**

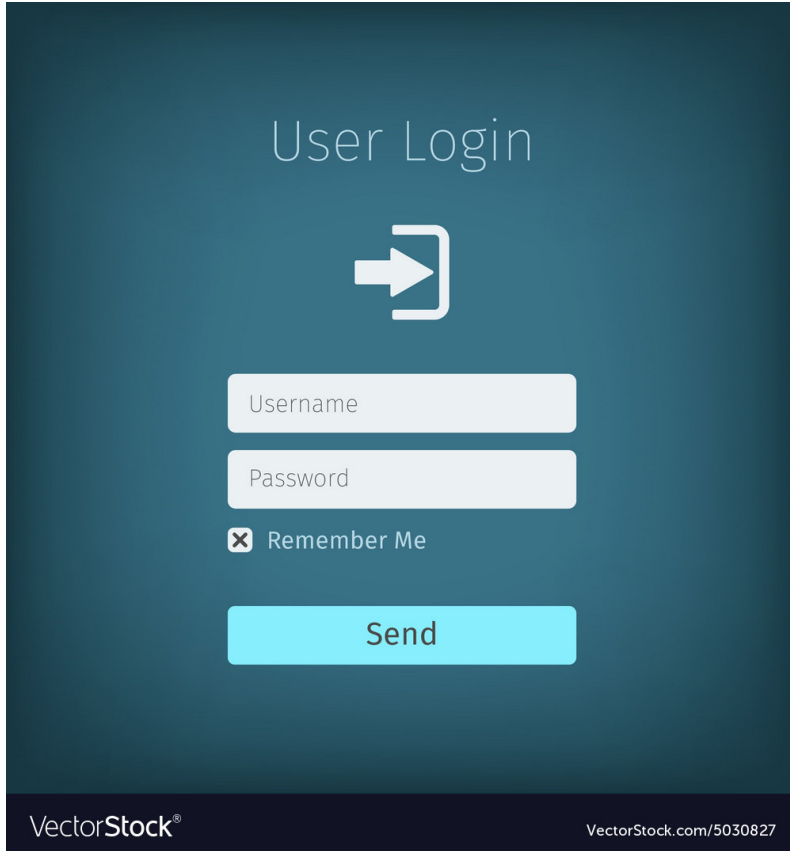
Identify Security Risk: Login Portals



A mockup of a user login form on a dark teal background. The form includes the text "User Login" at the top, a white icon of an arrow pointing into a bracket, two input fields labeled "Username" and "Password", a checkbox labeled "Remember Me" which is checked, and a bright cyan "Send" button. At the bottom, there is a "VectorStock" logo and a URL "VectorStock.com/5030827".

- /login
- /wp-login
- /admin
- /portal

Identify Security Risk: Brute Force Logins

A dark blue login form titled "User Login" with a white icon of an arrow pointing into a bracket. It contains two input fields for "Username" and "Password", a checkbox labeled "Remember Me" which is checked, and a light blue "Send" button. The bottom of the form has "VectorStock®" and "VectorStock.com/5030827" in small white text.

User Login

➔

Username

Password

☒ Remember Me

Send

VectorStock®

VectorStock.com/5030827

- admin:password
- admin:password1
- admin:letmein
- admin:secret
- admin:12345678
- admin:rocky
- admin:password!

Proactive Strategy: Bloody Trapland

1. Insert honeypot areas/code
2. Send an alert from the application if the honeypot is triggered
3. Block the offending user/source IP

Robots.txt

- Add a fake entry to robots.txt that blocks any user that visits it

```
← → ↻ https://facebook.com/robots.txt

# Notice: Collection of data on Facebook through automated means is
# prohibited unless you have express written permission from Facebook
# and may only be conducted for the limited purpose contained in said
# permission.
# See: http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: Applebot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /plugins/
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?
```

Fake Cookies

Filter Items			
Name	Value	Domain	Path
isAdmin	false	www.amegala.com	/

Cookie: isAdmin=False

Fake JavaScript Comments

```
40 <body>
41   <div class="sb-site-container">
42     <div class="boxed">
43       <header id="header-full-top" class="header-full-dark">
44         <div class="container">
45           <div class="header-full-title">
46             <h1>
47               <a href="/">
48                 Nebraska.Code()
49               </a>
50             </h1>
51             <p>July 13-15, 2022</p>
52           </div>
53           <nav class="top-nav hidden-xs">
54             <div class="dropdown animated fadeInDown">
55               <a href="/Account/Login">Login / Register</a>
56             </div><!-- previous login portal at /account/login/old needs to be removed as it doesn't have brute force protection -->
57
58             <ul class="top-nav-social hidden-sm">
59               <li><a href="https://twitter.com/amegala" class="animated fadeIn animation-delay-7 twitter"><i class="fa fa-twitter"></i></a></li>
60               <li><a href="https://www.facebook.com/amegalaconferences/" class="animated fadeIn animation-delay-8 facebook"><i class="fa fa-facebook"></i></a></li>
61             </ul>
```

Inserted comment: “previous login portal at /account/login/old needs to be removed as it doesn’t have brute force protection”

Fake URL Parameters

The screenshot shows a web browser with the address bar displaying `https://nebraskacode.amegala.com/?adminView=false`. The website header features the Nebraska.Code() logo, the dates July 13-15, 2022, and a navigation menu with links: Home, Register, Pricing, Schedule, Sponsors, Scholarship, and About. The main content area has a dark background with a building at night. It includes the text "Nebraska.Code() is back!" followed by a list of bullet points: "A plethora of sessions covering all software development tools, stacks, and technologies!", "Your opportunity to advance your career", and "Legendary social and networking events". Below the list are two buttons: "Sponsorship Opportunities" and "View Sessions". On the right side, there is a large Nebraska.Code() logo and text stating "Nebraska.Code: July 14th - 15th" and "Pre-Conference Workshops: July 13th".

https://nebraskacode.amegala.com/?adminView=false

Nebraska.Code()
July 13-15, 2022

Login / Register

an Amegala conference

Home Register Pricing Schedule Sponsors Scholarship About

Nebraska.Code() is back!

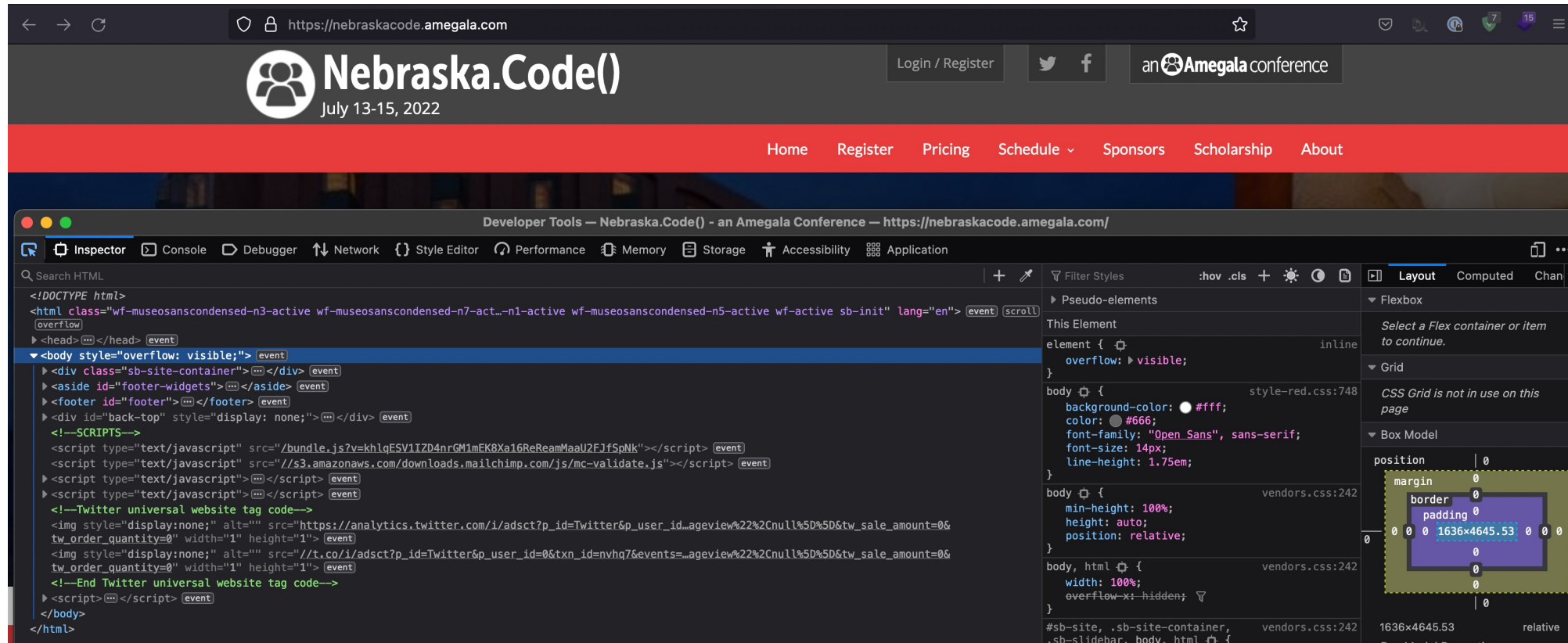
- > A plethora of sessions covering all software development tools, stacks, and technologies!
- > Your opportunity to advance your career
- > Legendary social and networking events

Sponsorship Opportunities

View Sessions

Nebraska.Code()
Nebraska.Code: July 14th - 15th
Pre-Conference Workshops: July 13th

Developer Tools



Only two types of users utilize developer tools: developers and hackers

Threat Modeling

Script
Kiddie



Targeted
Attacker



Opportunistic
Attacker

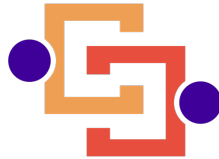
\$\$\$

Nation
State
Threat



Threat Modeling

- Eliminate threats of low-level attackers
- Give security more time to focus on advanced attackers



Questions?



nathaniel.shere@craftcompliance.com



<https://www.linkedin.com/in/nathaniel-shere/>