Craft Compliance

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

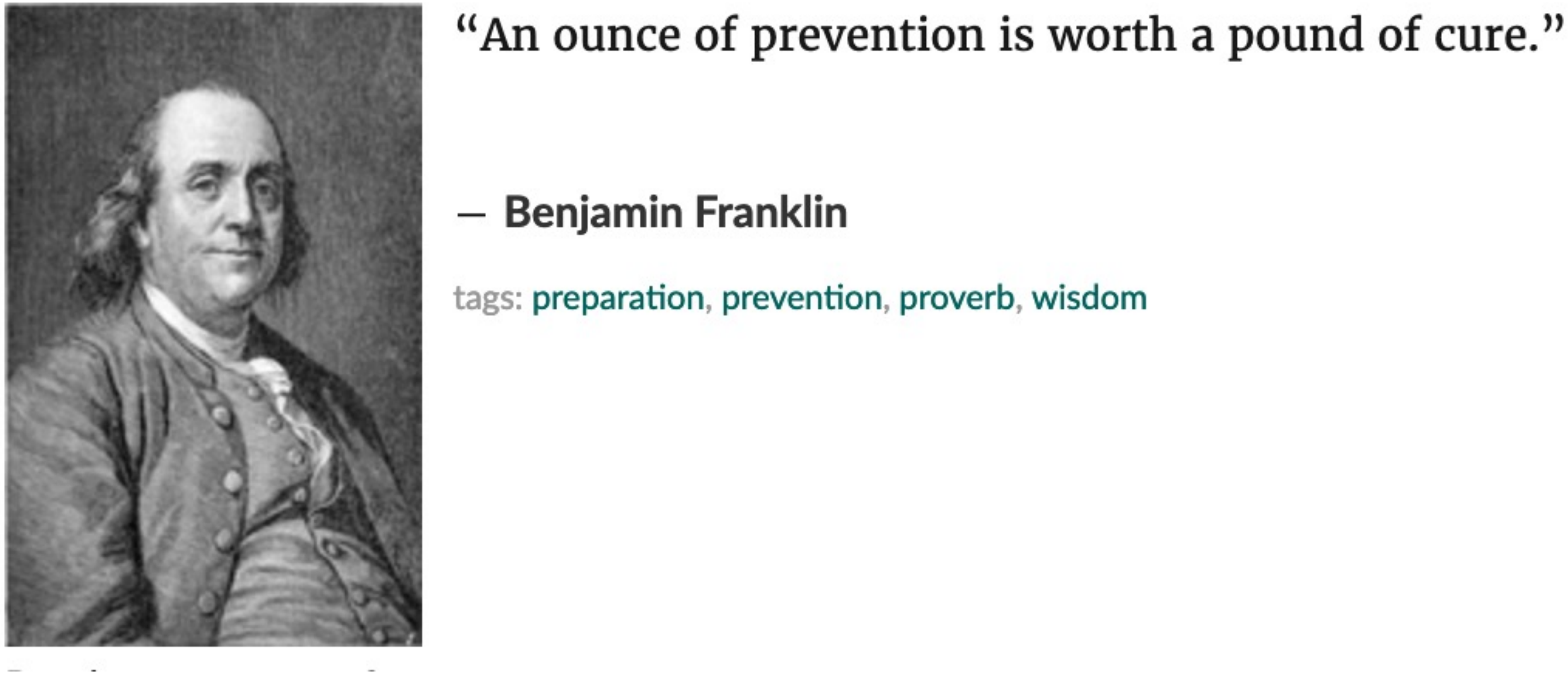
What I Will Cover

- 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

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

80

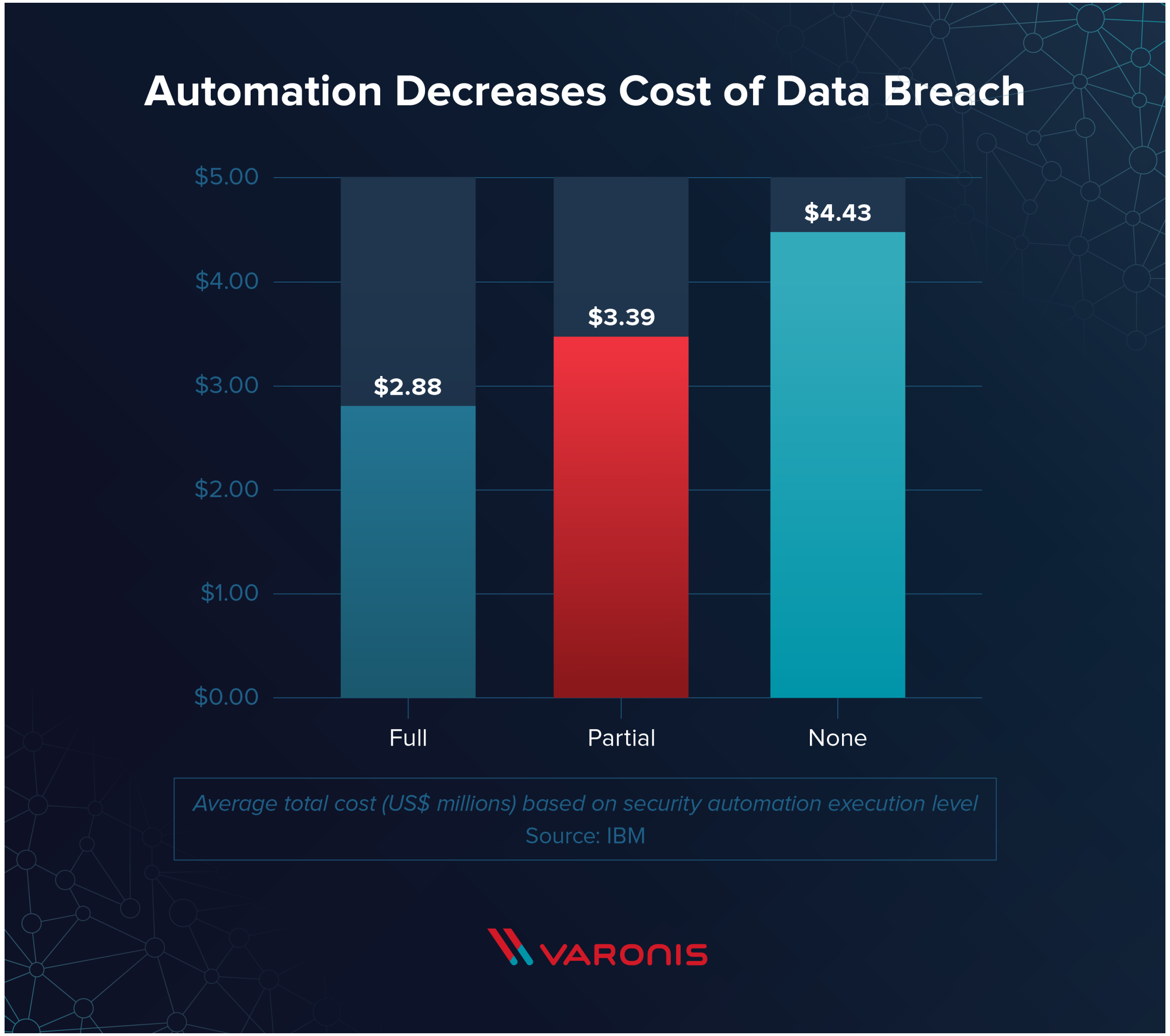
The average time (days) to contain a breach in 2020

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

367

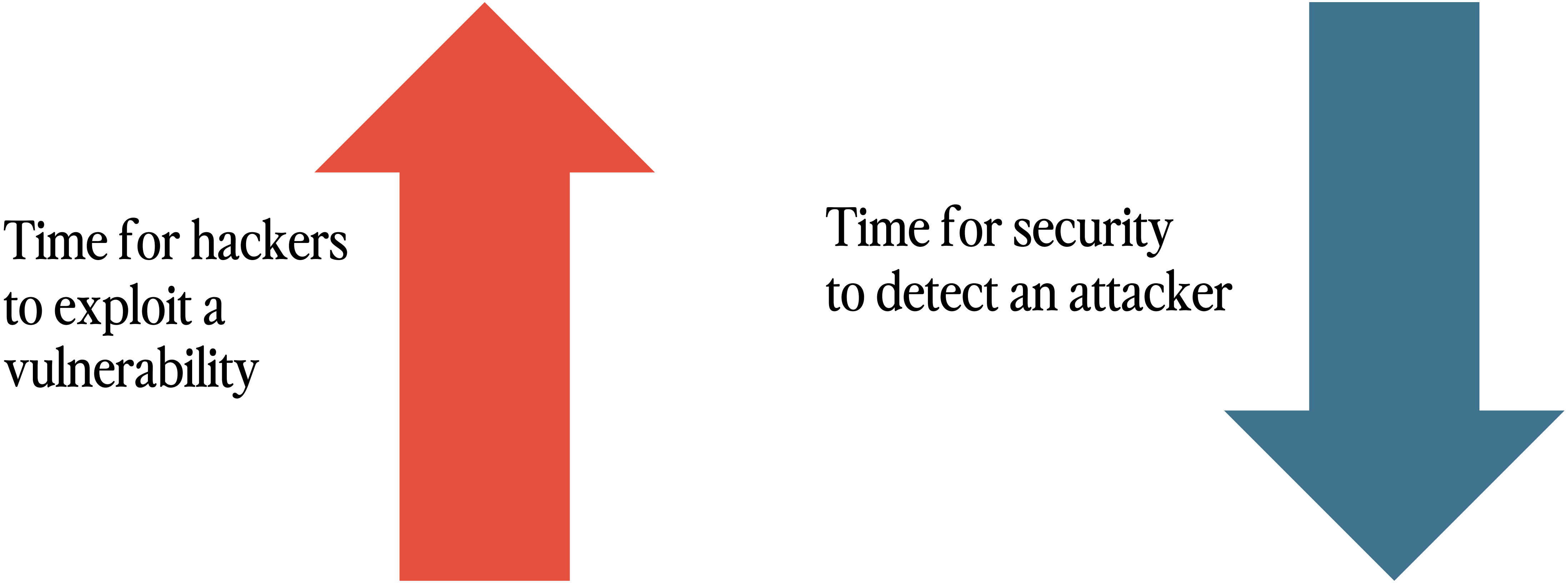
The average length (days) of a breach in 2020

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



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

Security Goals



Time for hackers to exploit a vulnerability

Time for security to detect an attacker

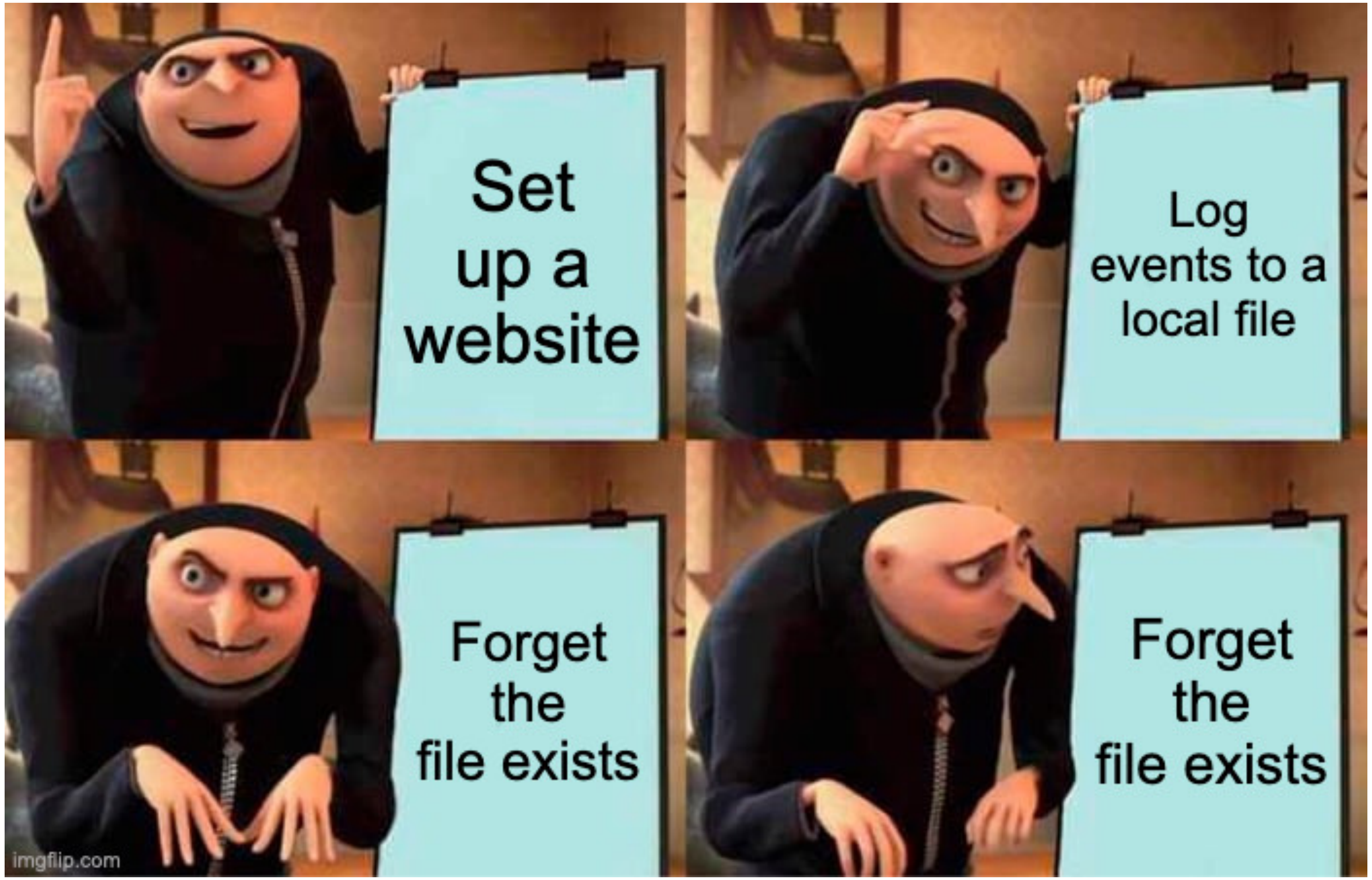
Security Strategies

- Reactive
- Proactive

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)

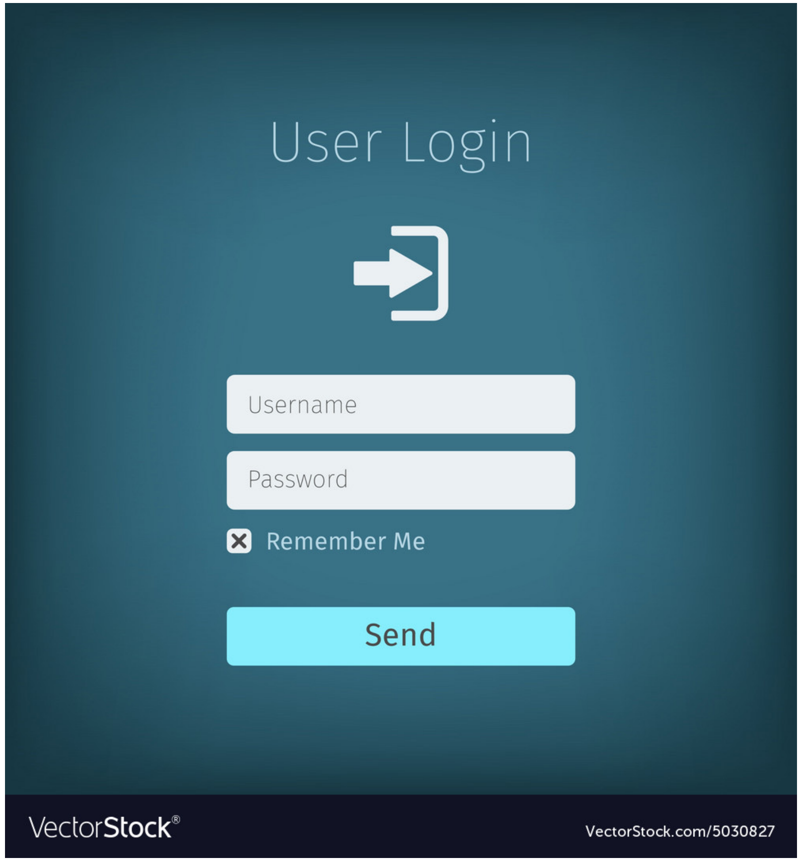
1. Implement logging
2. Collect logs in centralized place
3. Add rules and correlation logic to logs
4. Implement alerting based on triggers and thresholds
5. Identify stakeholders and asset owners
6. Create triage steps and playbooks for each alert
7. Add rules and correlation logic to alerts
8. Implement 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

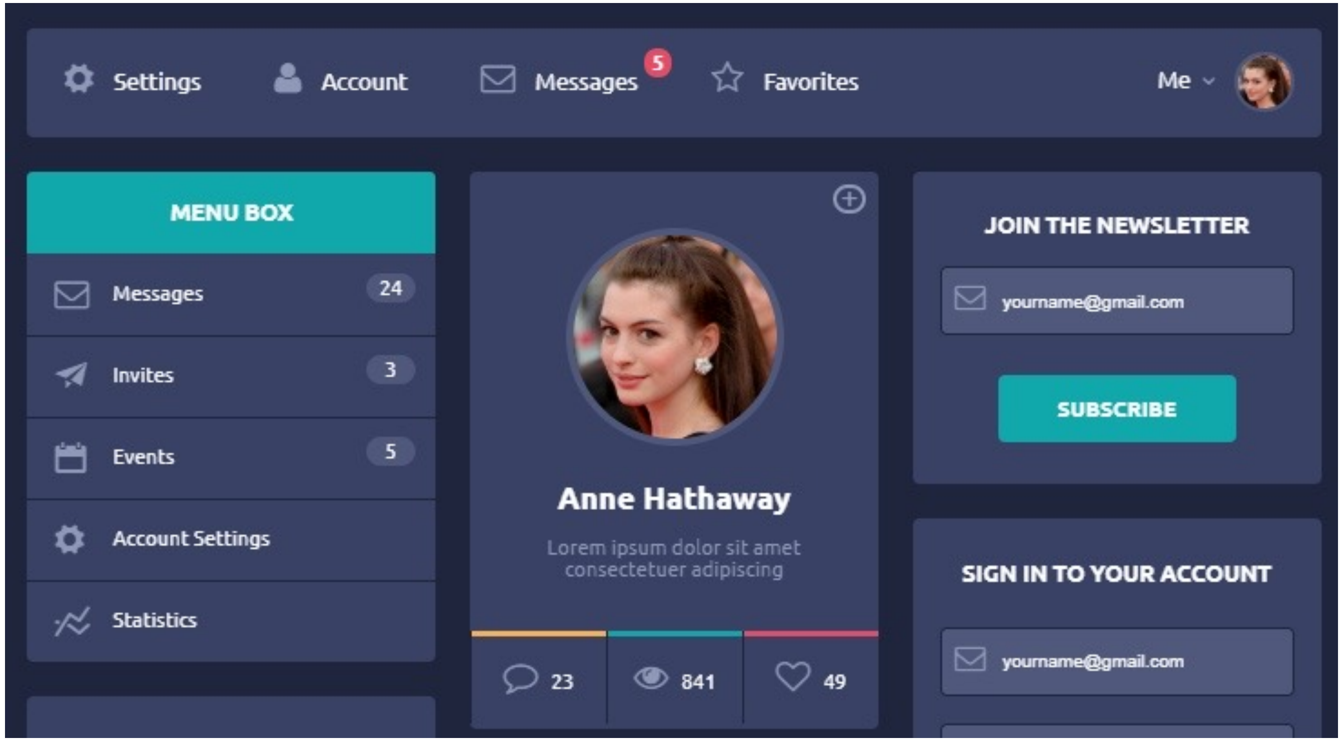
1. Identify a security risk in your application
2. Send an alert from the application if the risk is triggered
3. Block the offending user/source IP
   - Table of blocked sources
   - Automated request to WAF

Brute Forcing Login Portal



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

Data Enumeration



Anne Hathaway

Lorem ipsum dolor sit amet consectetuer adipiscing

GET /users/4/profile

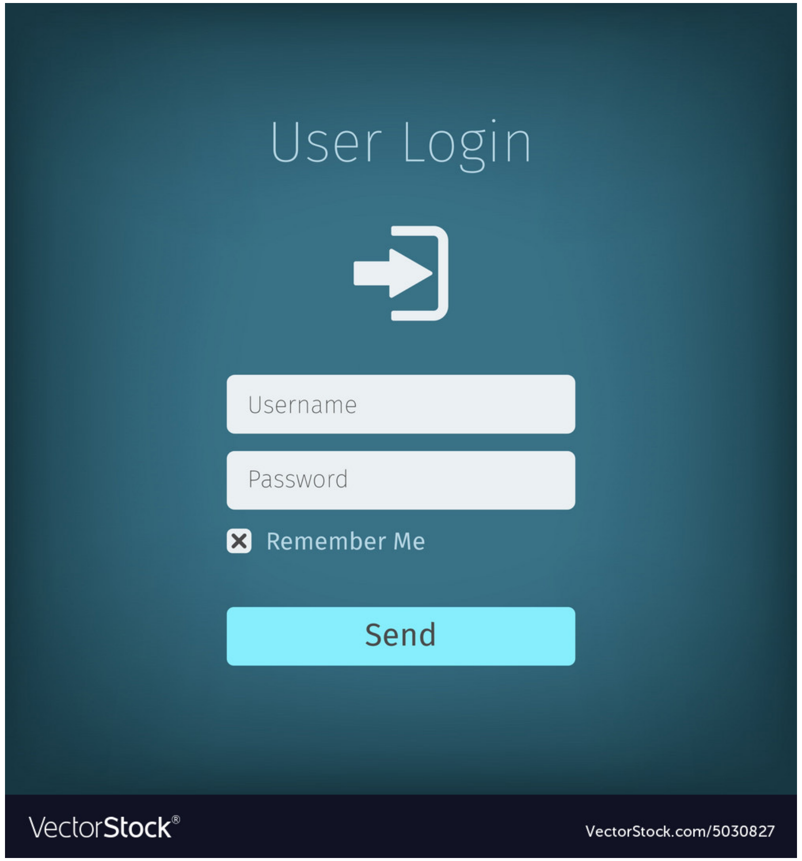
Data Enumeration

GET /users/4/profile

GET /client/75/edit

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

User Searching for Backend Login Portal

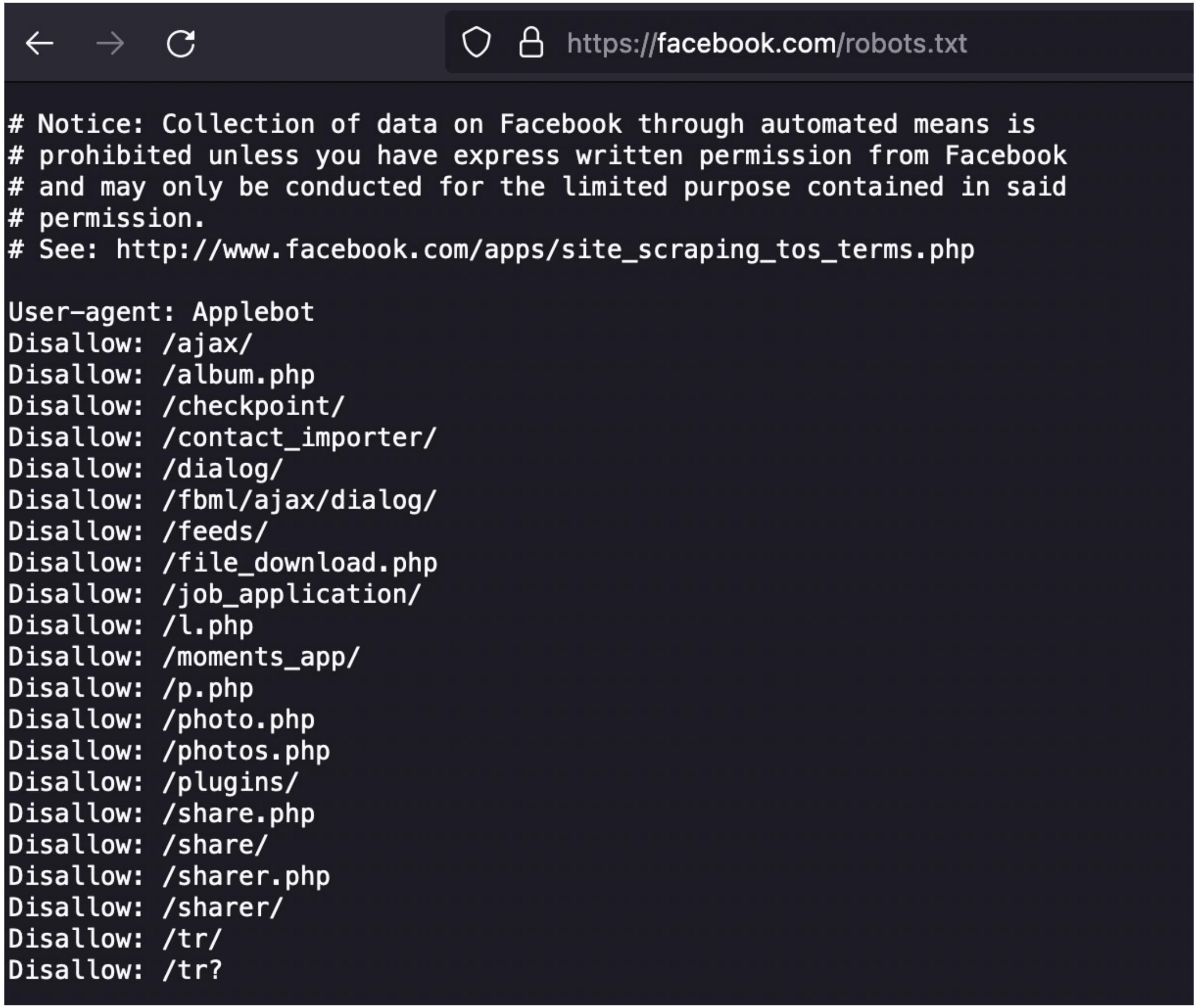


- /login
- /wp-login
- /admin
- /portal

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

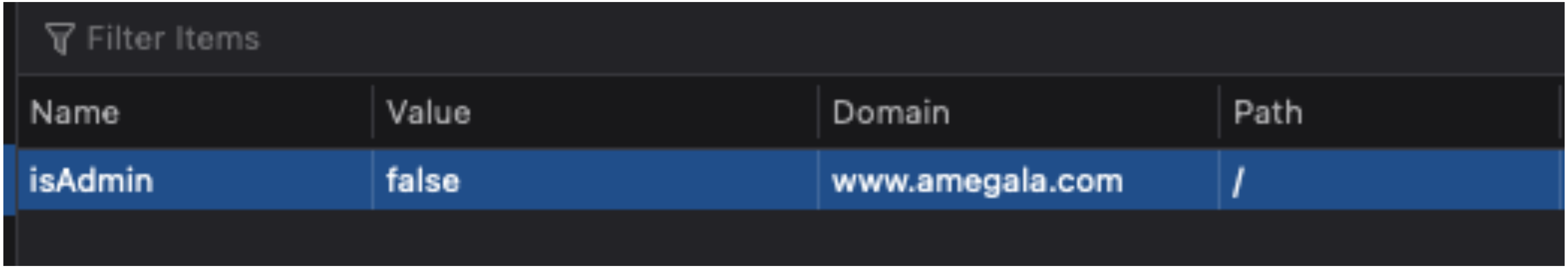
Robots.txt



```
# 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?
```

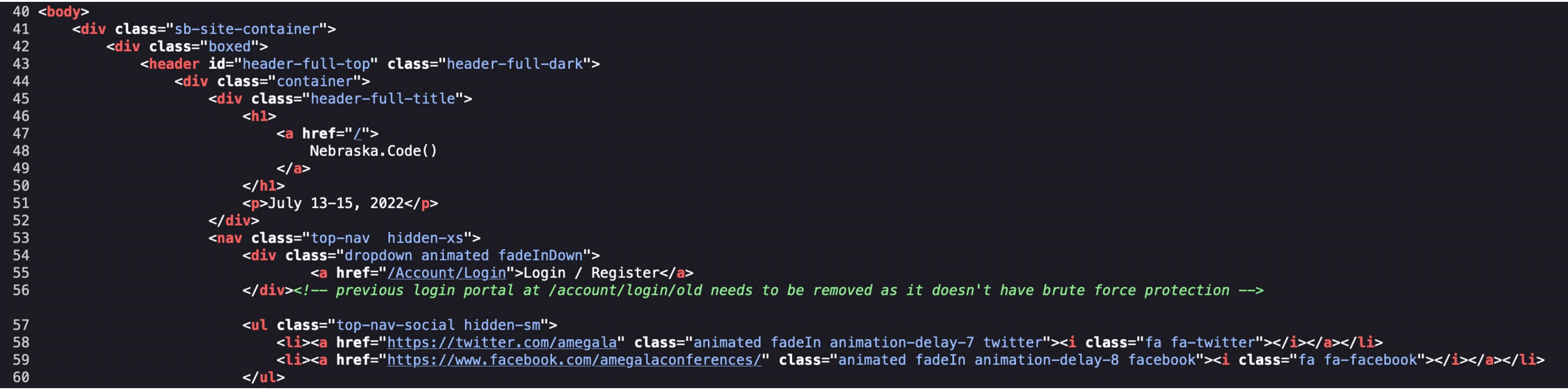
Fake Cookies



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

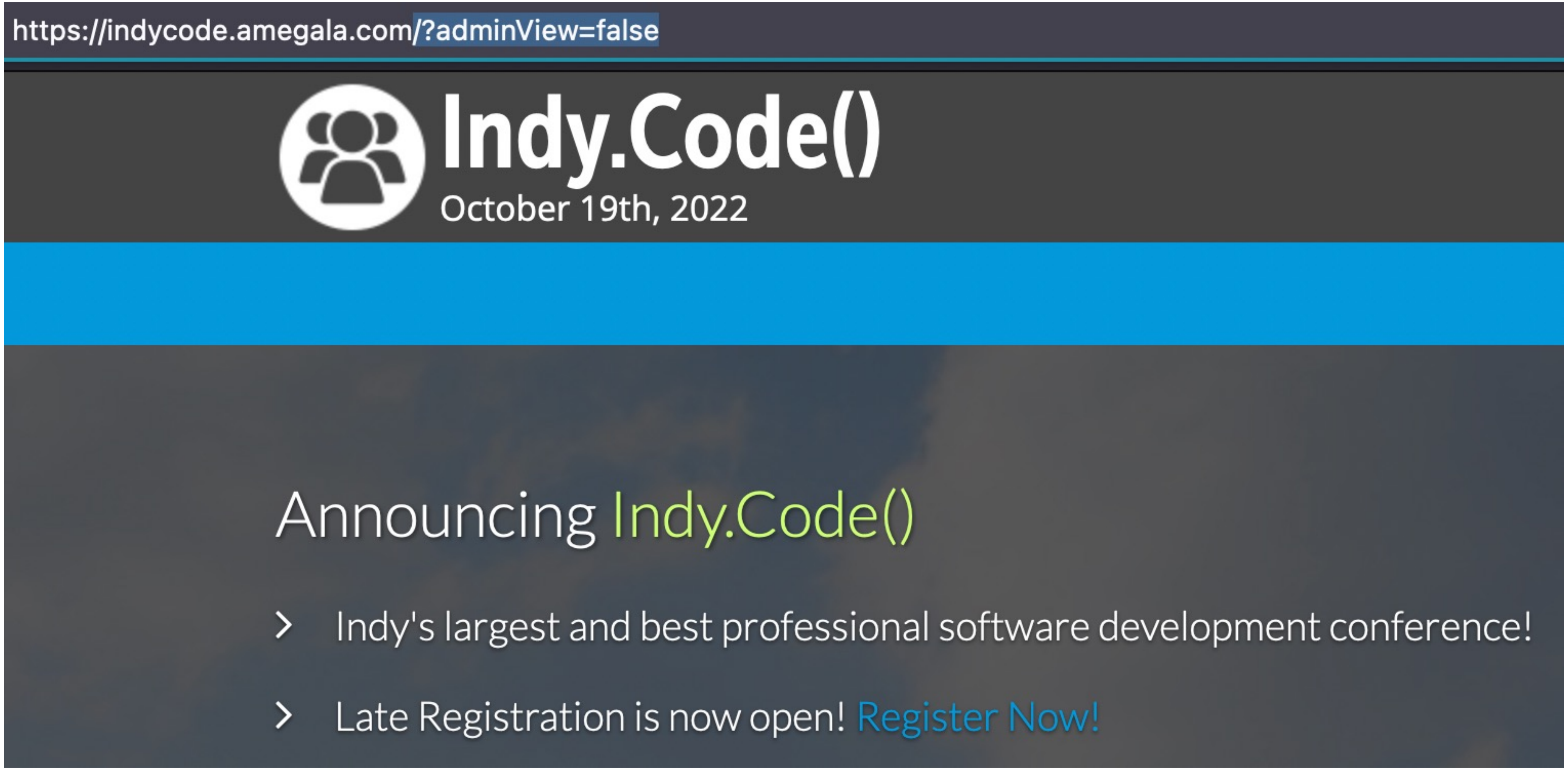
Cookie: isAdmin=False

Fake JavaScript Comments



```
<body>
    <div class="sb-site-container">
        <div class="boxed">
            <header id="header-full-top" class="header-full-dark">
                <div class="container">
                    <div class="header-full-title">
                        <h1>
                            <a href="/">
                                Nebraska.Code()
                            </a>
                        </h1>
                        <p>July 13-15, 2022</p>
                    </div>
                    <nav class="top-nav  hidden-xs">
                        <div class="dropdown animated fadeInDown">
                                <a href="/Account/Login">Login / Register</a>
                        </div><!-- previous login portal at /account/login/old needs to be removed as it doesn't have brute force protection -->
                        <ul class="top-nav-social hidden-sm">
                            <li><a href="https://twitter.com/amegala" class="animated fadeIn animation-delay-7 twitter"><i class="fa fa-twitter"></i></a></li>
                            <li><a href="https://www.facebook.com/amegalaconferences/" class="animated fadeIn animation-delay-8 facebook"><i class="fa fa-facebook"></i></a></li>
                        </ul>
```

Fake URL Parameters



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

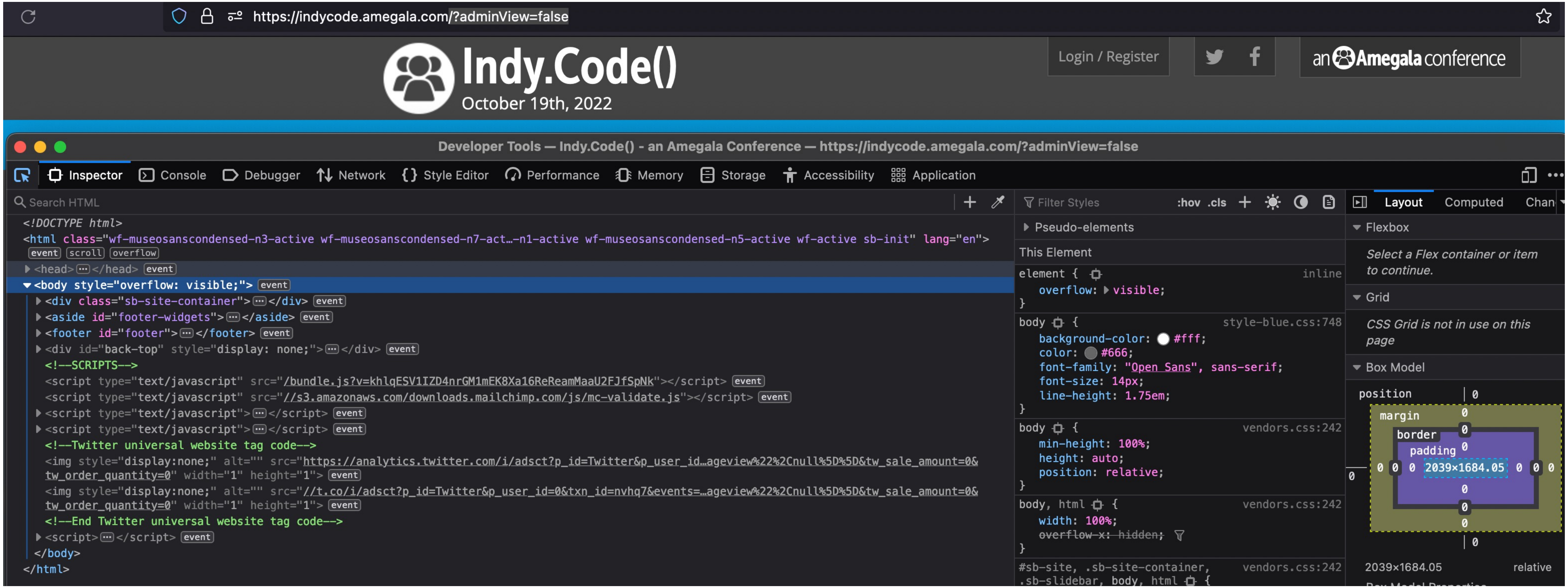
Indy.Code()

October 19th, 2022

Announcing Indy.Code()

- Indy's largest and best professional software development conference!
- Late Registration is now open! Register Now!

Developer Tools



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

Developer Tools — Indy.Code() - an Amegala Conference — https://indycode.amegala.com/?adminView=false

```
<!DOCTYPE html>
<html class="wf-museosanscondensed-n3-active wf-museosanscondensed-n7-act…-n1-active wf-museosanscondensed-n5-active wf-active sb-init" lang="en">
 event  scroll  overflow
  <head>…</head> event
  <body style="overflow: visible;"> event
    <div class="sb-site-container">…</div> event
    <aside id="footer-widgets">…</aside> event
    <footer id="footer">…</footer> event
    <div id="back-top" style="display: none;">…</div> event
    <!--SCRIPTS-->
    <script type="text/javascript" src="/bundle.js?v=khlqESV1IZD4nrGM1mEK8Xa16ReReamMaaU2FJfSpNk"></script> event
    <script type="text/javascript" src="//s3.amazonaws.com/downloads.mailchimp.com/js/mc-validate.js"></script> event
    <script type="text/javascript">…</script> event
    <script type="text/javascript">…</script> event
    <!--Twitter universal website tag code-->
    <img style="display:none;" alt="" src="https://analytics.twitter.com/i/adsct?p_id=Twitter&p_user_id…ageview%22%2Cnull%5D%5D&tw_sale_amount=0&
    tw_order_quantity=0" width="1" height="1"> event
    <img style="display:none;" alt="" src="//t.co/i/adsct?p_id=Twitter&p_user_id=0&txn_id=nvhq7&events=…ageview%22%2Cnull%5D%5D&tw_sale_amount=0&
    tw_order_quantity=0" width="1" height="1"> event
    <!--End Twitter universal website tag code-->
    <script>…</script> event
  </body>
</html>
```

Pseudo-elements

This Element

```
element {                                   inline
   overflow: visible;
}
body {                          style-blue.css:748
   background-color: #fff;
   color: #666;
   font-family: "Open Sans", sans-serif;
   font-size: 14px;
   line-height: 1.75em;
}
body {                             vendors.css:242
   min-height: 100%;
   height: auto;
   position: relative;
}
body, html {                       vendors.css:242
   width: 100%;
   ~~overflow-x: hidden;~~
}
#sb-site, .sb-site-container,      vendors.css:242
.sb-slidebar, body, html {
```

Flexbox

Select a Flex container or item to continue.

Grid

CSS Grid is not in use on this page

Box Model

2039×1684.05 relative

Threat Modeling

Script Kiddie

Targeted Attacker

Opportunistic Attacker

$$$

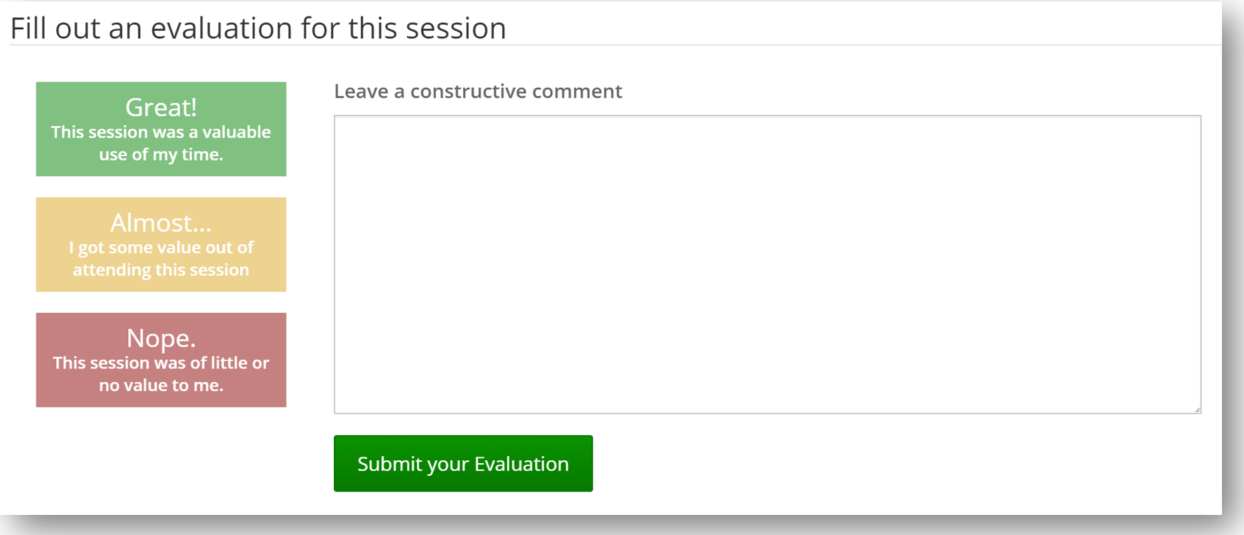
Nation State Threat

Questions?

✉ nathaniel.shere@craftcompliance.com

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

Get the slides: https://www.craftcompliance.com/presentations



Fill out an evaluation for this session

Great!
This session was a valuable use of my time.

Almost...
I got some value out of attending this session

Nope.
This session was of little or no value to me.

Leave a constructive comment

Submit your Evaluation

NebraskaCode.amegala.com/Schedule