SANS | OFFENSIVE OPERATIONS

Accidental Bug Discovery

(a.k.a. Solid Job Security for the Foreseeable Future)

Looks around. "Yeah, I could rob this place."

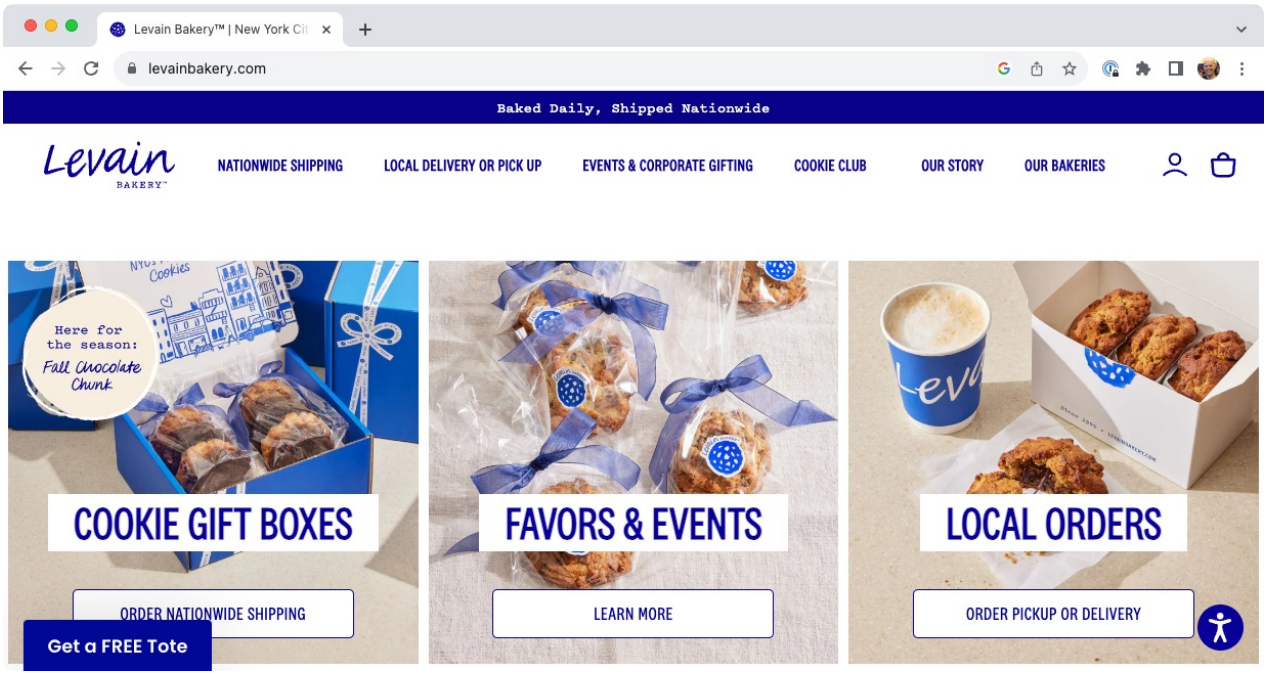
Hi, I'm Joshua Wright.

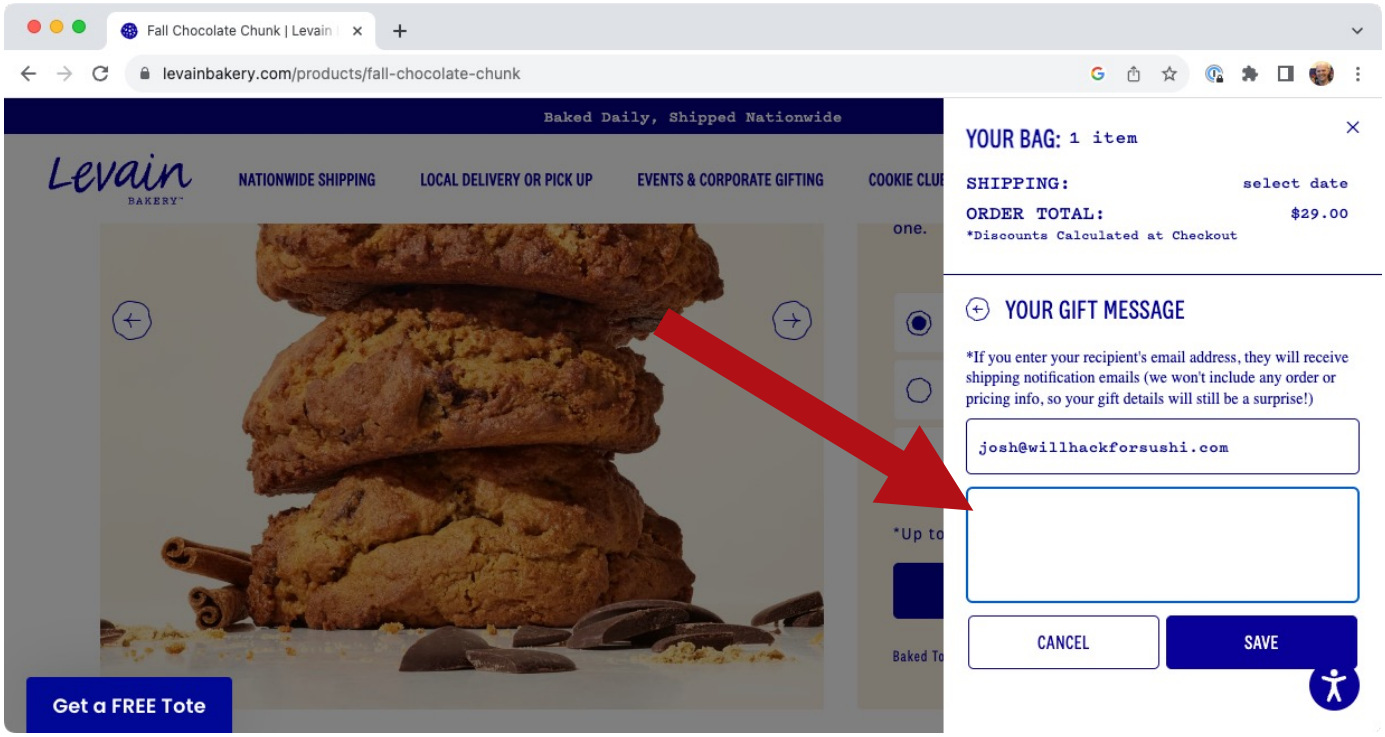
I write and teach SEC504 for SANS, and I hack for Counter Hack.

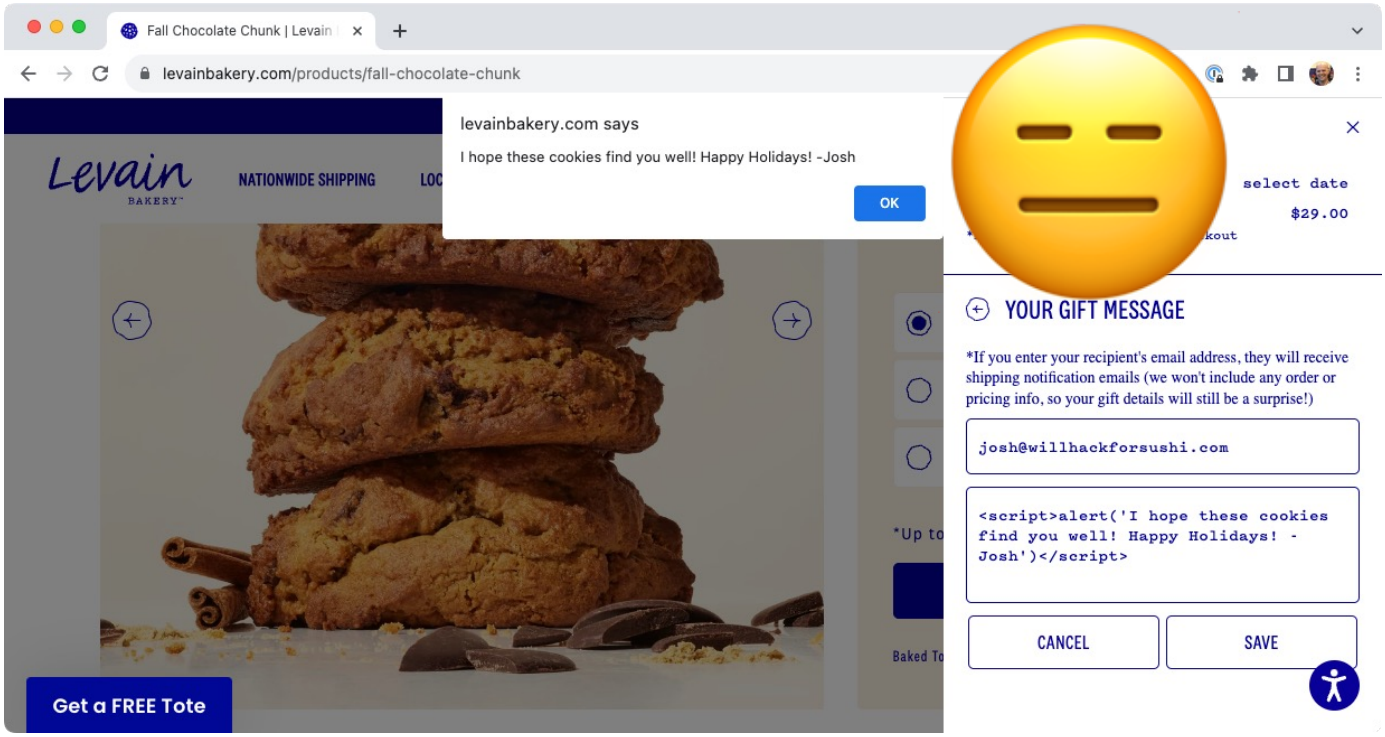
I have trouble browsing websites like a normal person.

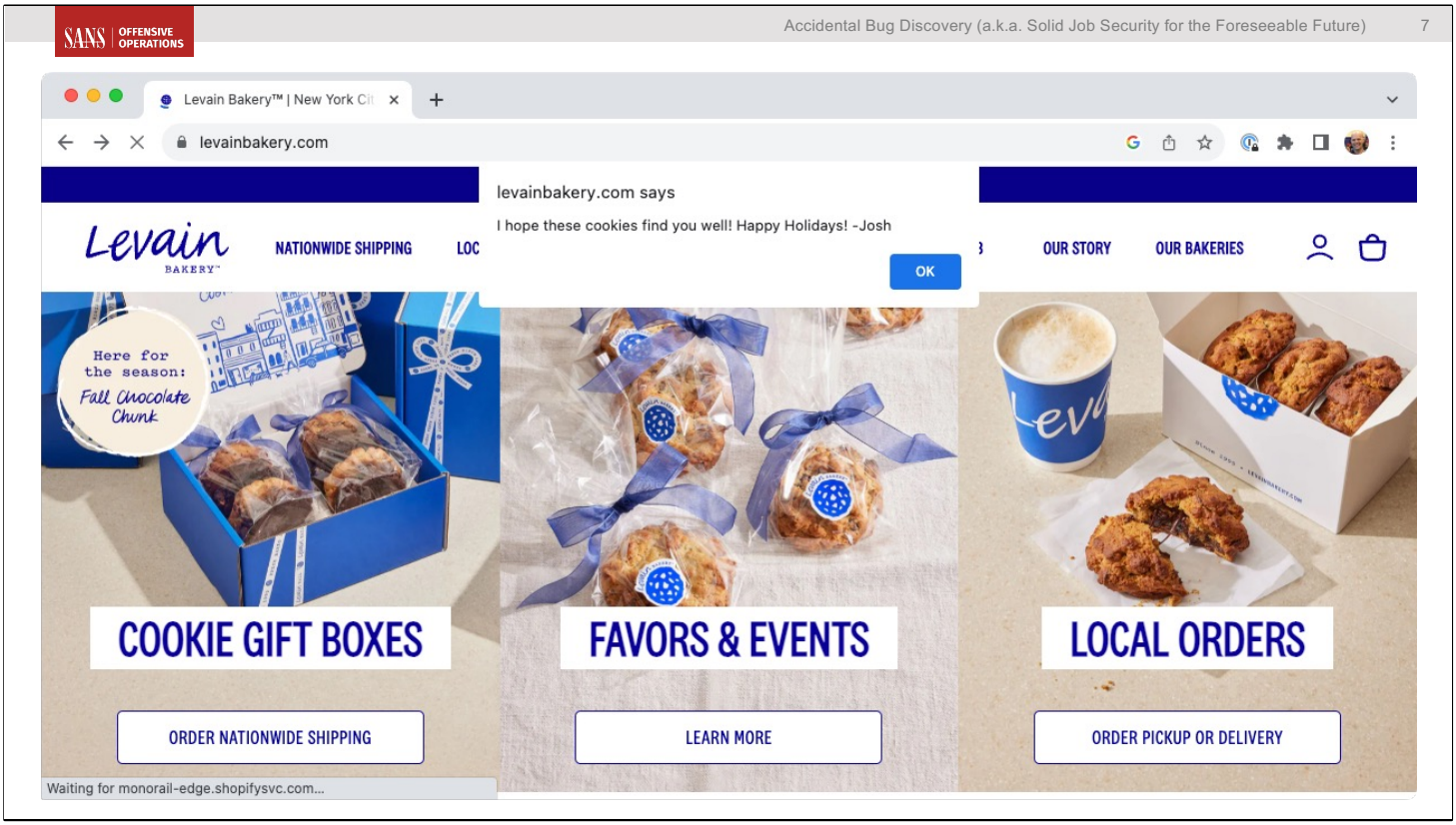
Here are three recent examples.

Sending Cookies as a Christmas Gift

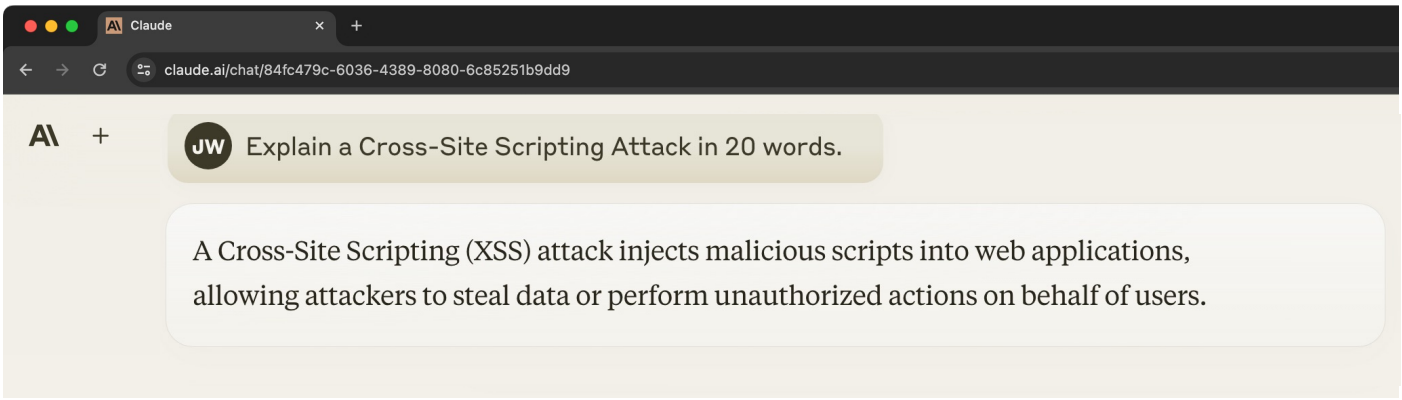


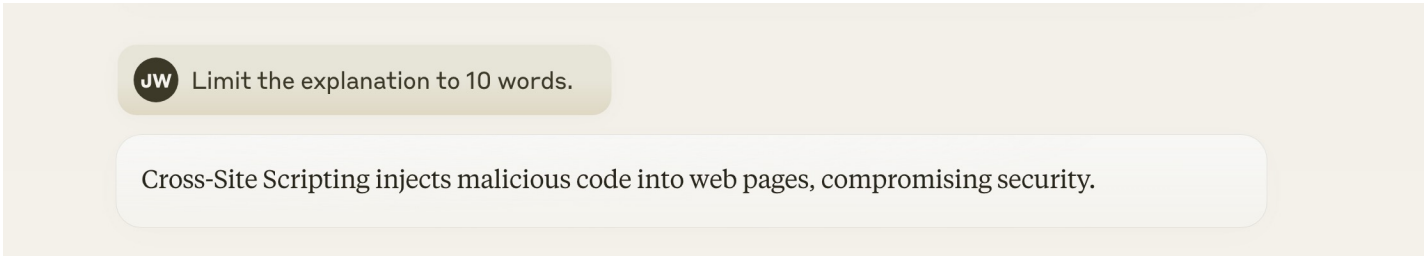

Fall Chocolate Chunk | Levain
levainbakery.com/products/fall-chocolate-chunk
Baked Daily, Shipped Nationwide
Levain
BAKERY
NATIONWIDE SHIPPING
LOCAL DELIVERY OR PICK UP
EVENTS & CORPORATE GIFTING
Get a FREE Tote
YOUR BAG: 1 item
SHIPPING: select date
ORDER TOTAL: $29.00
*Discounts Calculated at Checkout
YOUR GIFT MESSAGE
*If you enter your recipient's email address, they will receive shipping notification emails (we won't include any order or pricing info, so your gift details will still be a surprise!)
josh@willhackforsushi.com
CANCEL
SAVE


Fall Chocolate Chunk | Levain
levainbakery.com/products/fall-chocolate-chunk
levainbakery.com says
I hope these cookies find you well! Happy Holidays! -Josh
OK
Levain
BAKERY
NATIONWIDE SHIPPING
Get a FREE Tote
select date
$29.00
YOUR GIFT MESSAGE
*If you enter your recipient's email address, they will receive shipping notification emails (we won't include any order or pricing info, so your gift details will still be a surprise!)
josh@willhackforsushi.com
<script>alert('I hope these cookies find you well! Happy Holidays! -Josh')</script>
CANCEL
SAVE



Once delivered, the XSS continues in every single feature of the website.


Claude
claude.ai/chat/84fc479c-6036-4389-8080-6c85251b9dd9
JW
Explain a Cross-Site Scripting Attack in 20 words.
A Cross-Site Scripting (XSS) attack injects malicious scripts into web applications, allowing attackers to steal data or perform unauthorized actions on behalf of users.


JW
Limit the explanation to 10 words.
Cross-Site Scripting injects malicious code into web pages, compromising security.

JW Limit the explanation to 5 words.

Malicious code injection into websites.

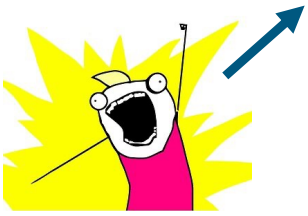
JW Limit the explanation to 1 word.

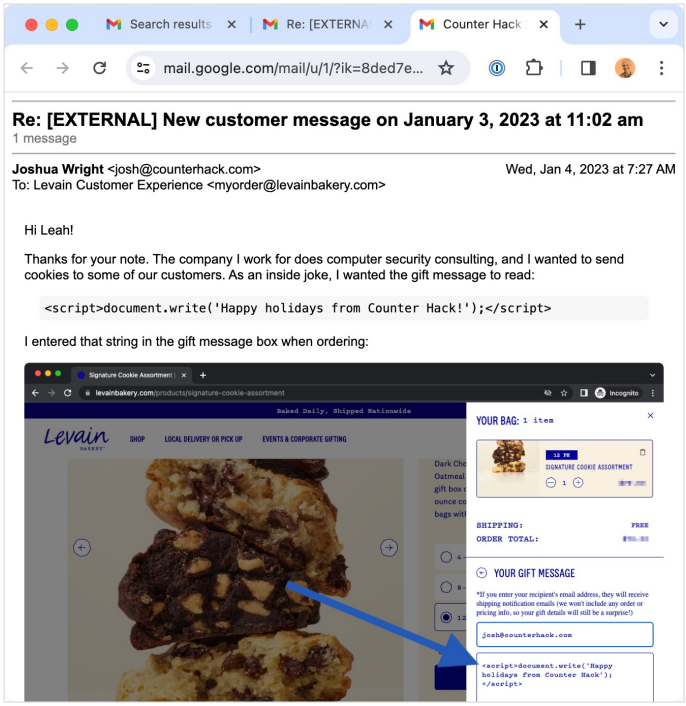
Hacksites.

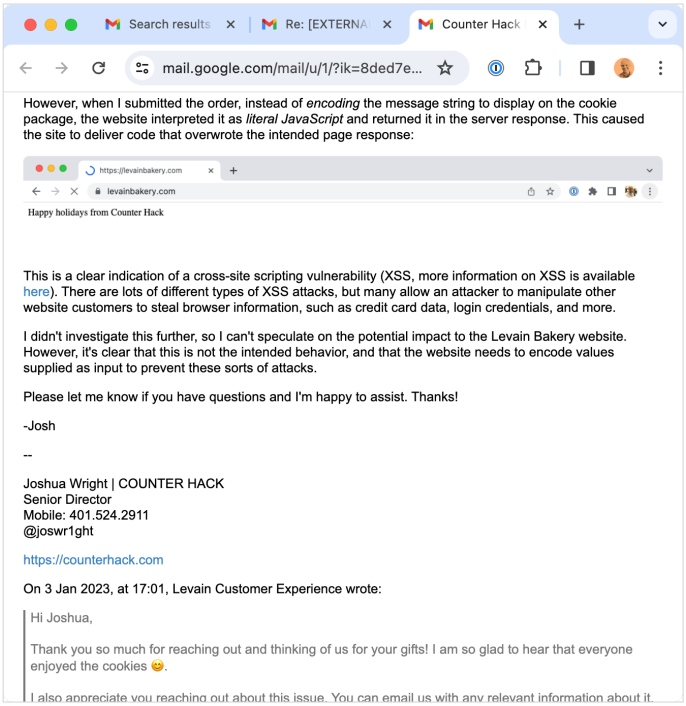
Copy

Subscribe to Pro and get **Claude 3 Opus**, our most intelligent model.

Subscribe to Pro





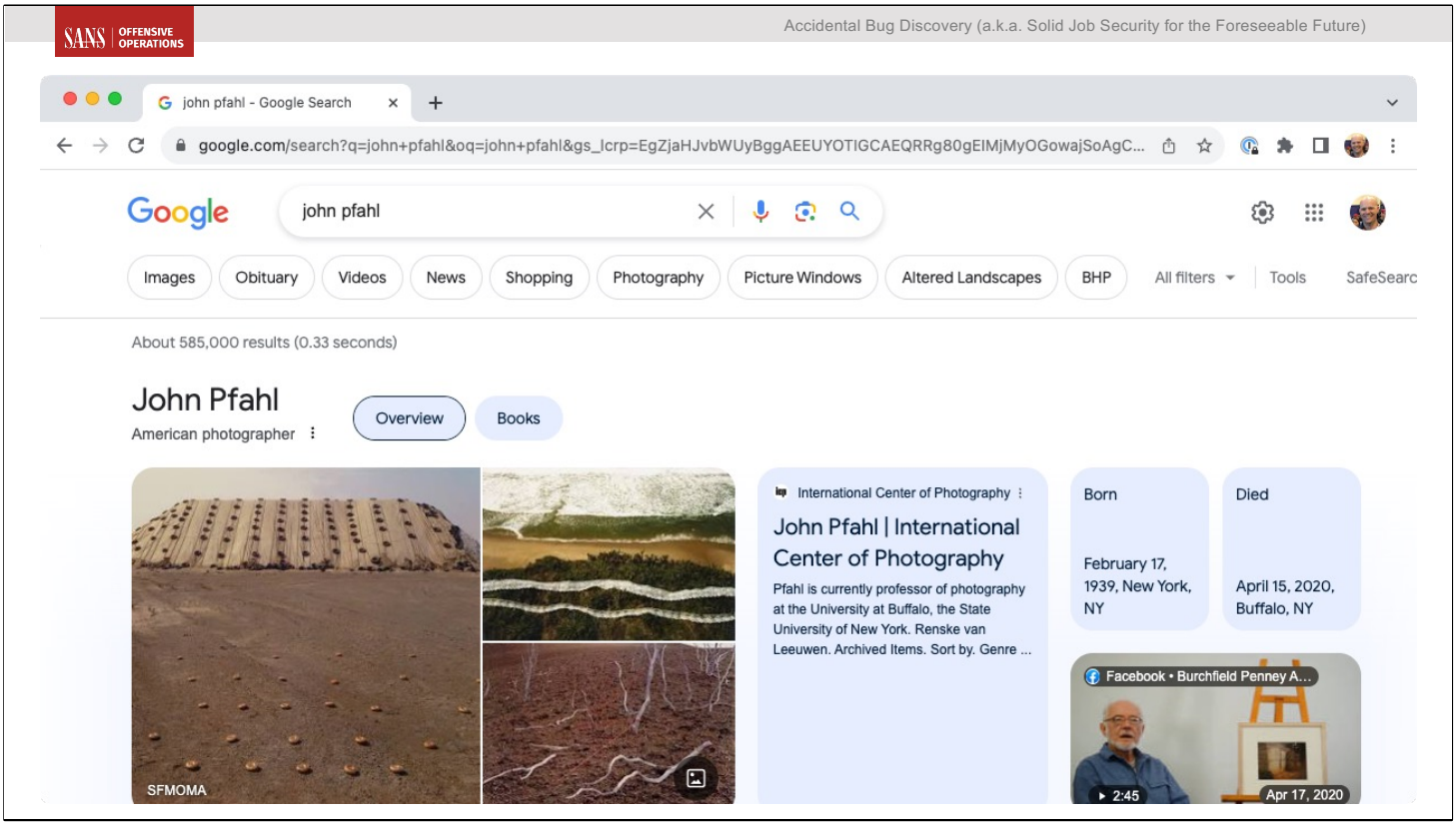


I reported the vulnerability in January 2023; still vulnerable.

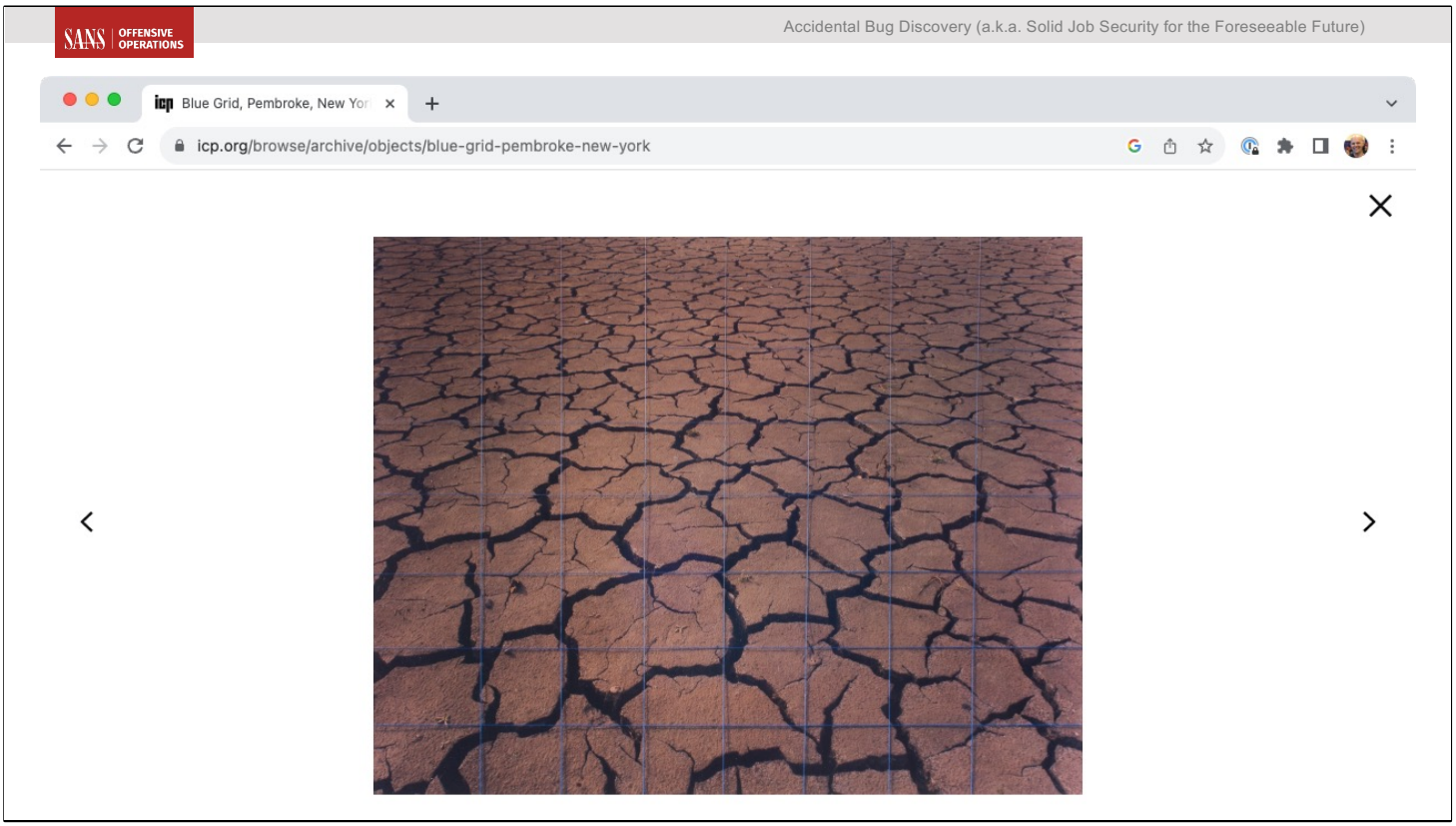
Levain Bakery Risk Assessment

- This could be a lowly *self-XSS* which might not even warrant remediation
- The lack of input/output validation in a form is an *indicator of future behavior* though, and concerning

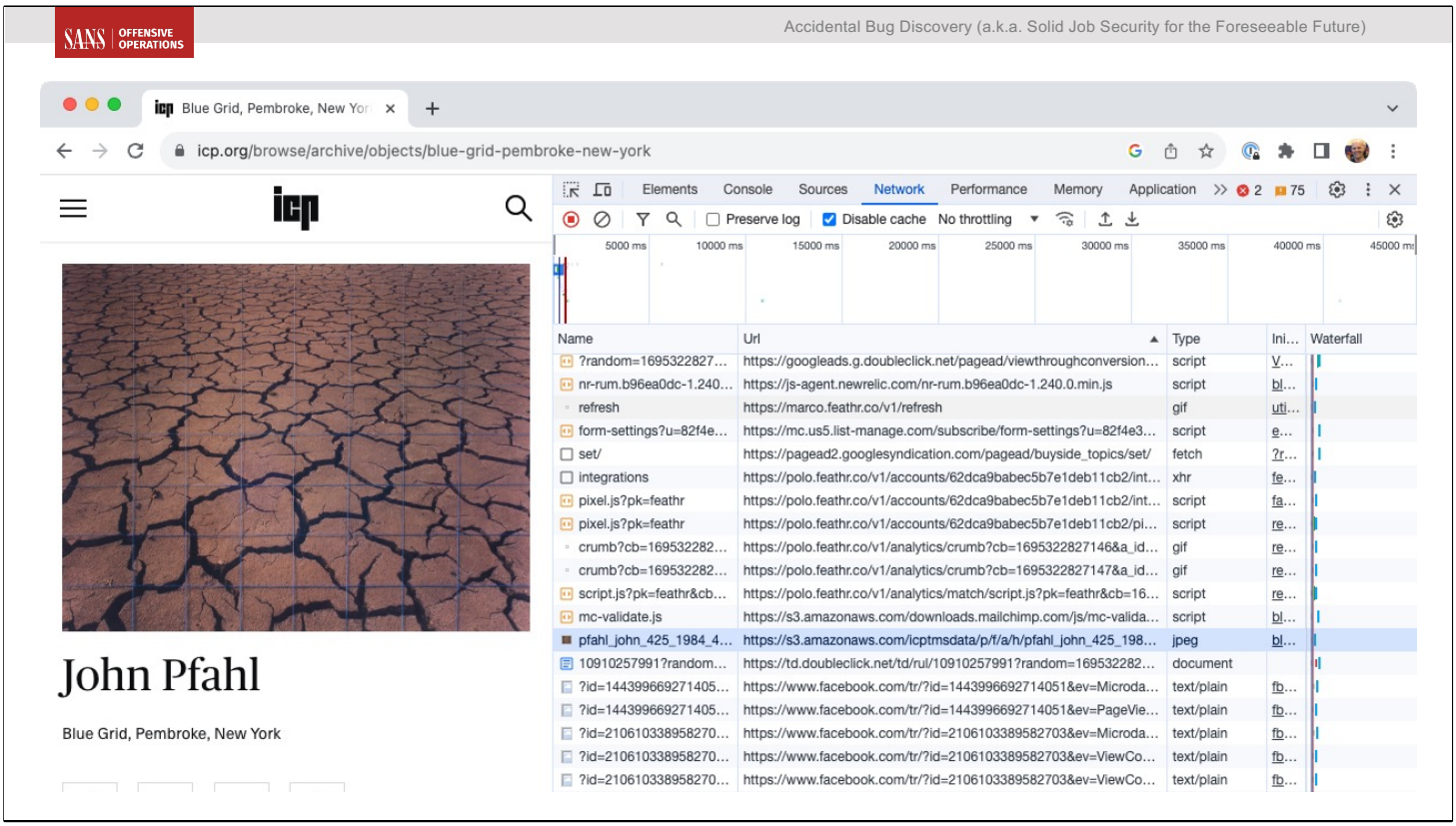
Even small companies with an online presence need to be responsive to security vulnerability reports. Casually entering <script> in a form should not trigger XSS vulnerabilities.



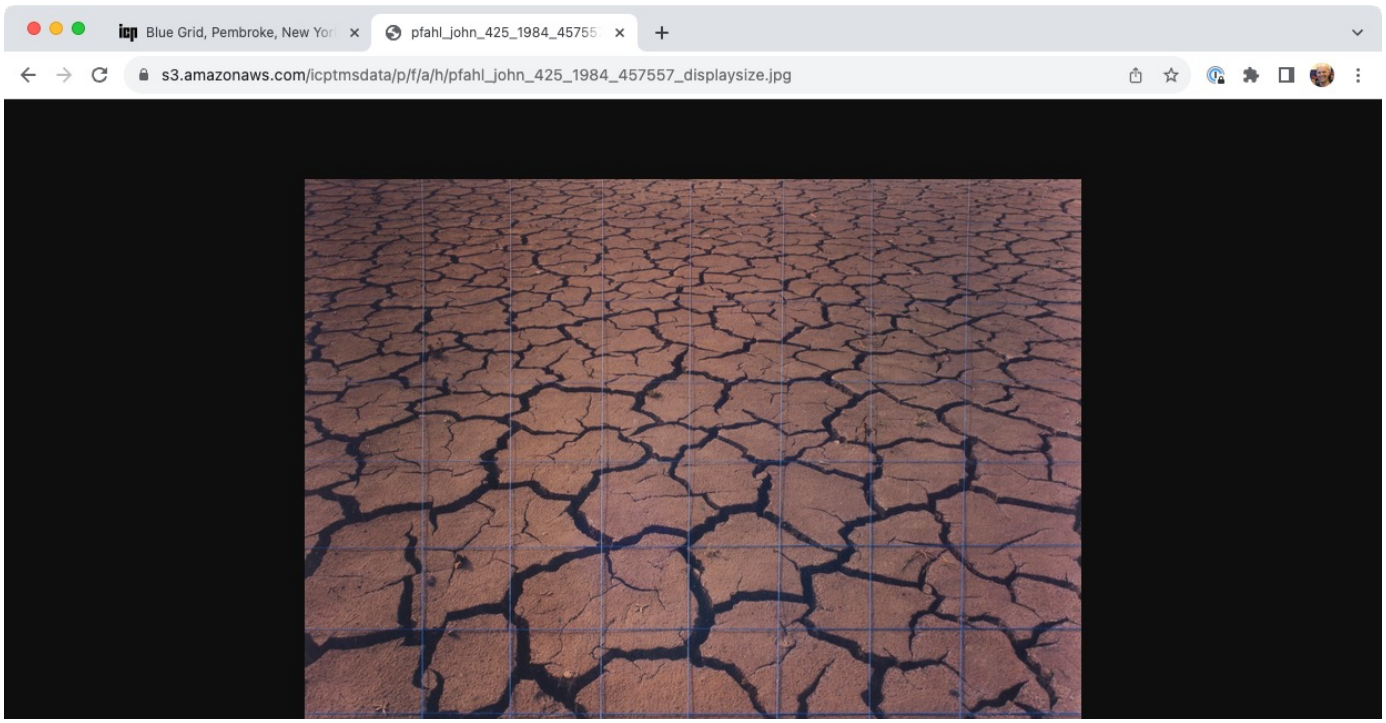
One day I wanted to find some of John Pfahl's photography. Google led me to the International Center of Photography (ICP) website.



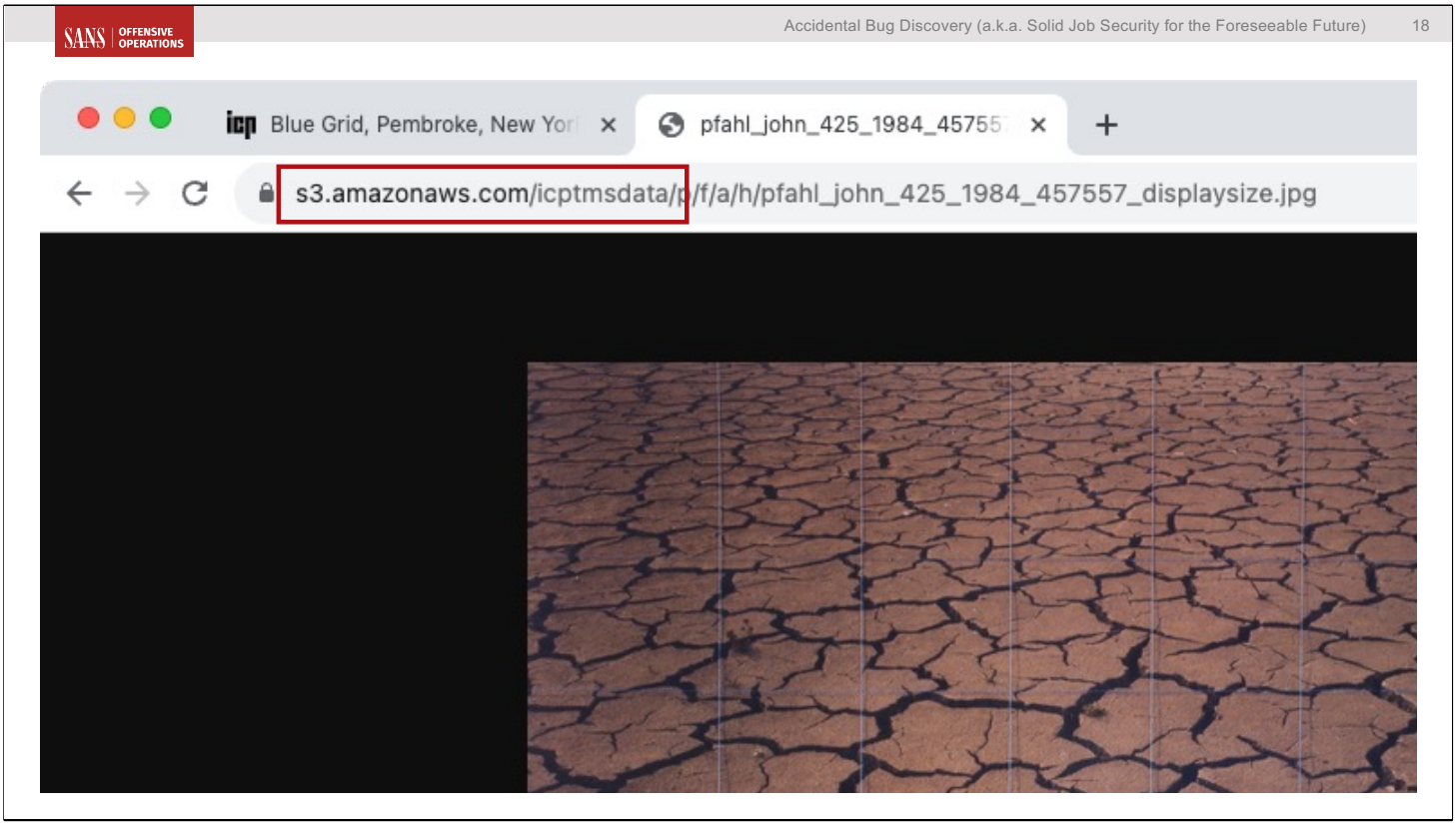
I wanted to look at this piece in full-screen mode, but the ICP website only allows me to view it in the lightbox view. Through JavaScript, ICP disables right-click support. :hugeeyeroll:



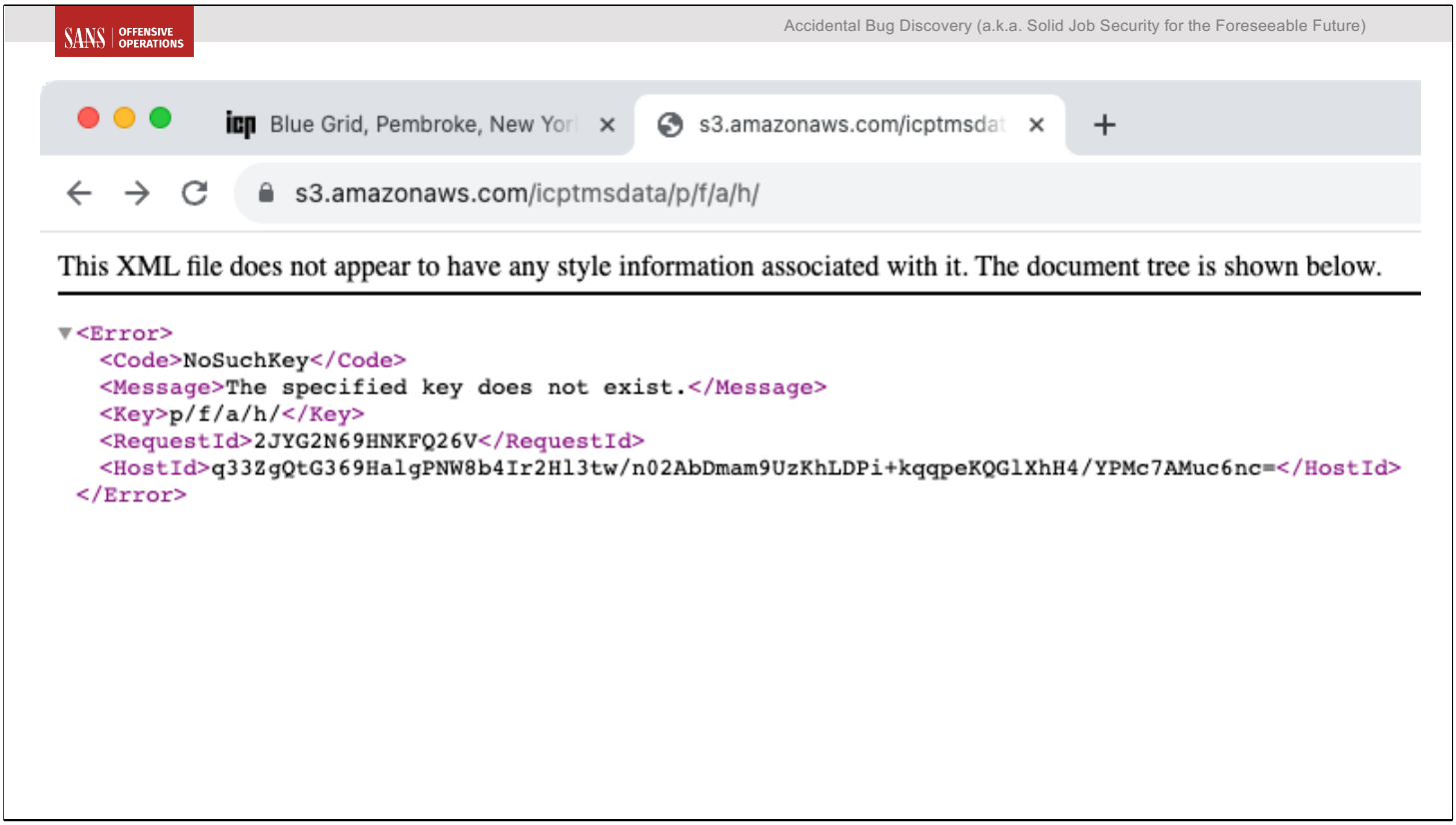
Opening developer tools, clicking the Network tab, and refreshing the page shows all the retrieved resources, including the image I want to see. From here I can open just the image in full screen.



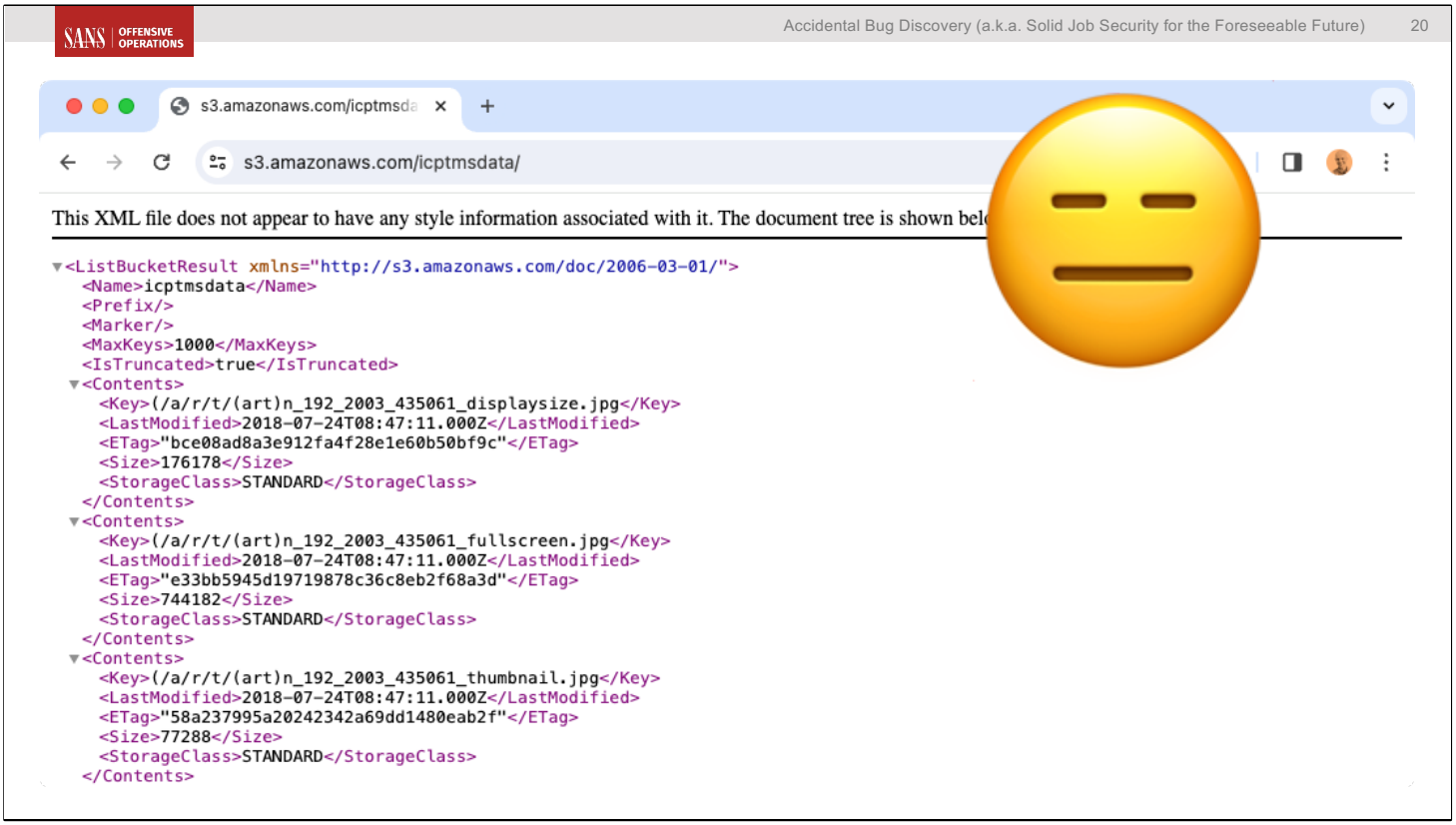
Full screen mode is all I wanted. But ... wait.



Well, now I need to investigate this S3 bucket.



Removing the file name from the URL doesn't display the contents of the bucket directory; this is normal for S3. Unlike a website that might have directory browsing turned on, S3 returns an error, because it's not like a "normal" file system.



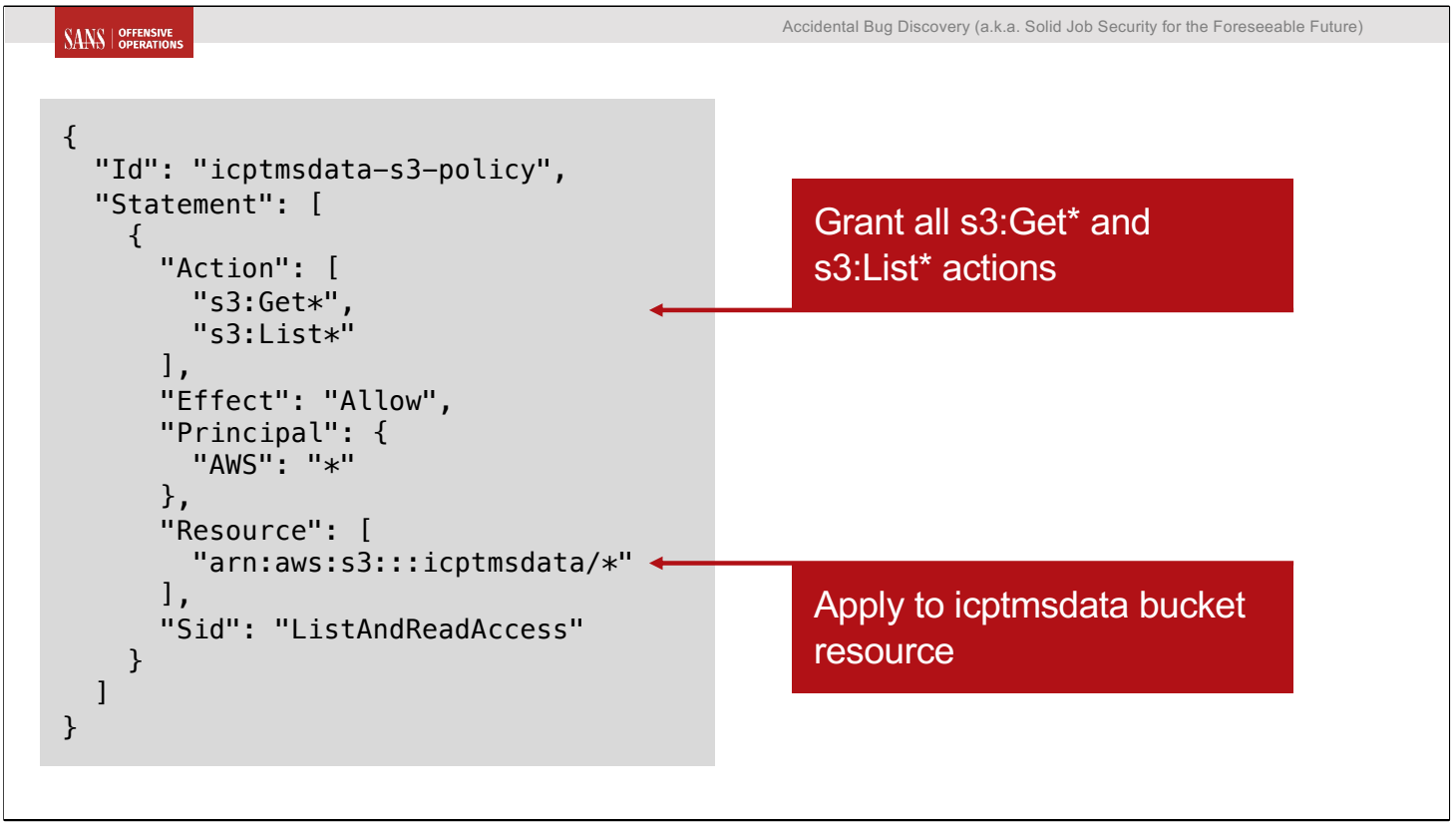
Browsing to the root of the bucket URL reveals XML data with all the file names, following the same path convention using several letters of the artist's last name (e.g., /p/f/a/h/).

```
~ $ aws sts get-caller-identity
{
    "UserId": "AIDAQ3GCTAHP6LLV6HZC2",
    "Account": "058390151647",
    "Arn": "arn:aws:iam::058390151647:user/jwright"
}
~ $ aws s3 ls s3://icptmsdata/p/f/a/h/
2018-07-24 10:11:21     419133 pfahl_john_1983_74_ii_413343_displaysize.jpg
2018-07-24 10:11:22    2529292 pfahl_john_1983_74_ii_413343_fullscreen.jpg
2018-07-24 10:11:22     120165 pfahl_john_1983_74_ii_413343_thumbnail.jpg
2018-07-24 10:11:22     585947 pfahl_john_1983_74_jj_460612_displaysize.jpg
2018-07-24 10:11:22    3515676 pfahl_john_1983_74_jj_460612_fullscreen.jpg
2018-07-24 10:11:22     159458 pfahl_john_1983_74_jj_460612_thumbnail.jpg
...
2018-07-24 10:13:30     149434 pfahl_john_altered_landscapes_13_464072_displaysize.jpg
2018-07-24 10:13:30    1154466 pfahl_john_altered_landscapes_13_464072_fullscreen.jpg
2018-07-24 10:13:30      44545 pfahl_john_altered_landscapes_13_464072_thumbnail.jpg
~ $ aws s3 ls s3://icptmsdata/p/f/a/h/ | wc -l
    1476
~ $ aws s3 ls --recursive s3://icptmsdata/ | wc -l
  333062
```

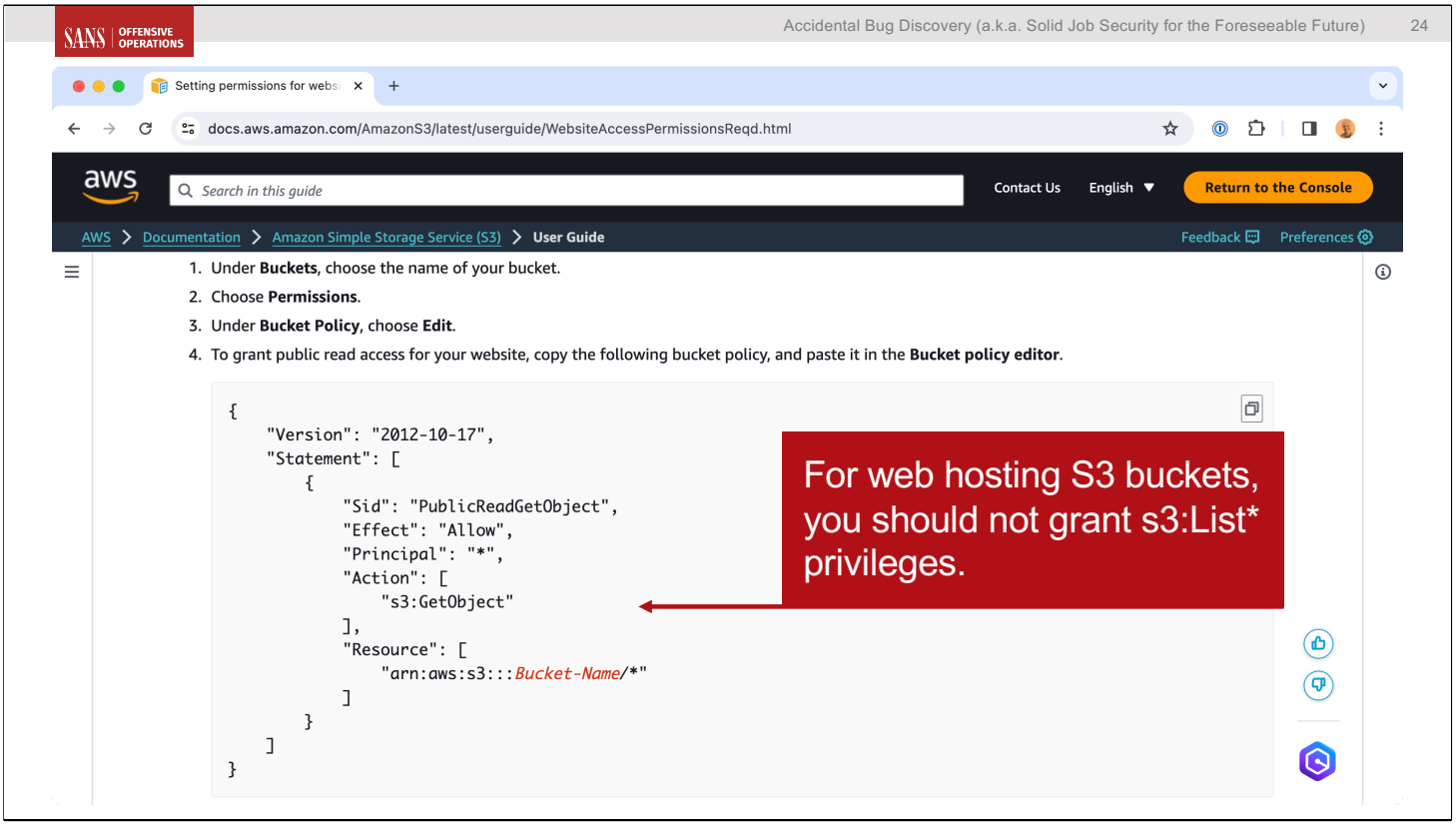
But the bucket data is more easily accessible using the AWS CLI utility. Here I'm using my own AWS credentials (for my *jwright* user) to access the ICP bucket, revealing hundreds of Pfahl's pieces in thumbnail to full resolution, including many not linked on the ICP website. What's more though, is that the photography for thousands of other artists is also disclosed – some 333,062 files.

```
~ $ aws s3 ls s3://icptmsdata/
                           PRE (/
                           PRE -/
                           PRE .bashrc.d/
                           PRE .profile.d/
                           PRE 0/
                           PRE 1/
                           PRE 2/
                           PRE 3/
                           PRE 6/
                           PRE 8/
                           PRE 9/
...
                           PRE z/
2018-07-24 09:26:20        220 .bash_logout
2018-07-24 09:26:20       2952 .bashrc
2018-07-24 09:26:20          0 .penv
2018-07-24 09:26:20        746 .profile
2018-07-25 04:20:27          0 .sdirs
```

Including a bunch of dotfiles for someone's presumably rsync'd home directory.



I don't have access to the ICP AWS IAM policies, but my guess is the S3 bucket is configured like the example shown here, where all users are granted s3:Get* and s3:List* actions.

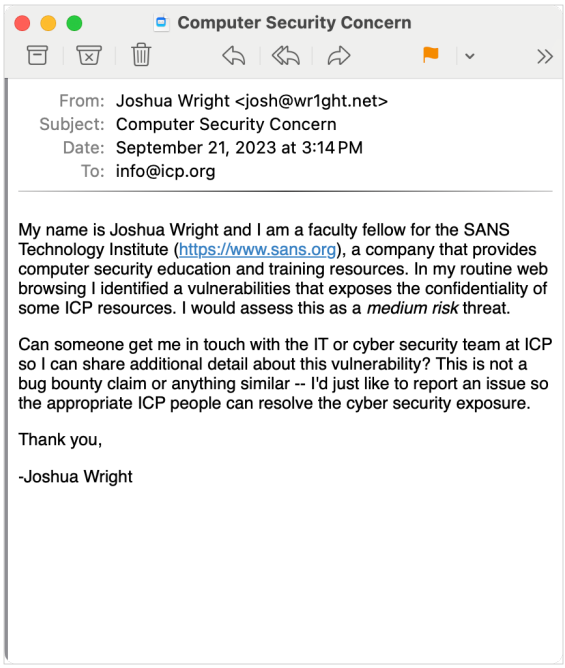


For web hosting though, they should not grant s3:List* privileges.

ICP Bucket Risk Assessment

- Bucket hosting website files: OK
- Bucket hosting all artwork including high-resolution files that is listable: *not OK*

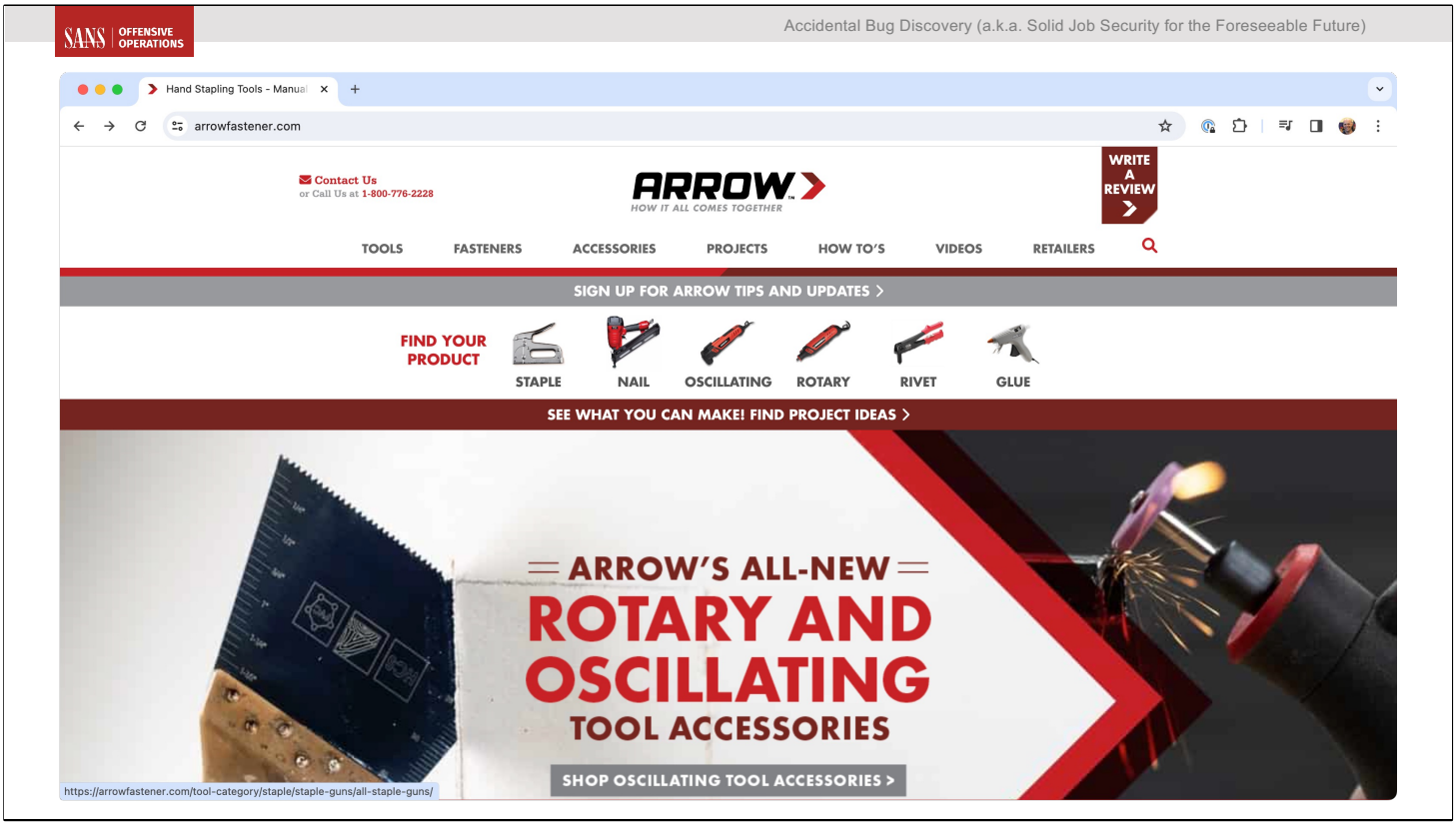
Risk assessment often requires understanding the business. A photographer who sends their original resolution pieces to ICP will likely be displeased with this vulnerability, allowing anyone to download and reproduce high-quality prints.



I've tried to report this vulnerability to ICP since September. No response.

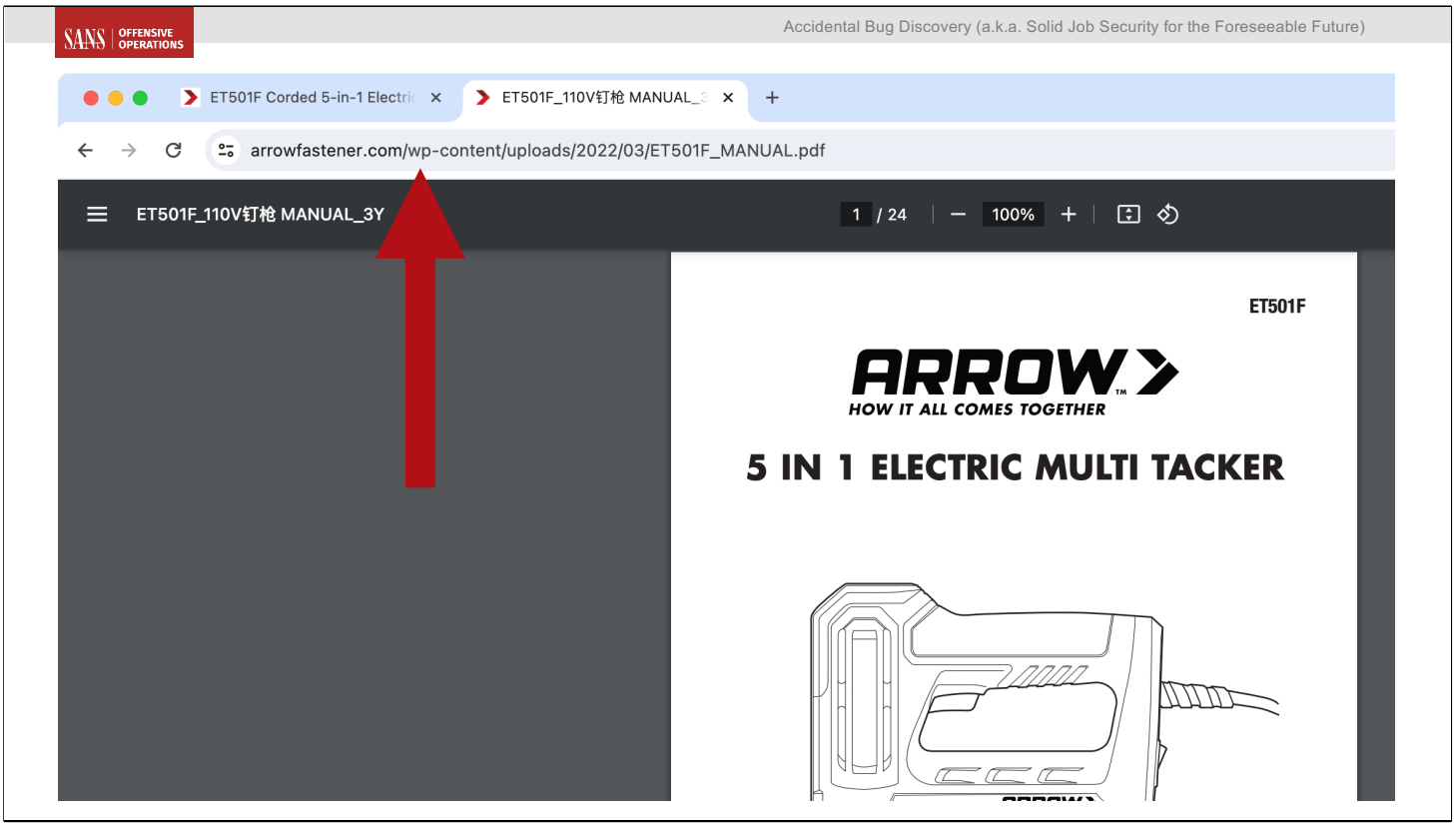
JW Explain the impact of sensitive information disclosure from an unprotected S3 bucket in one word.

Devastating.

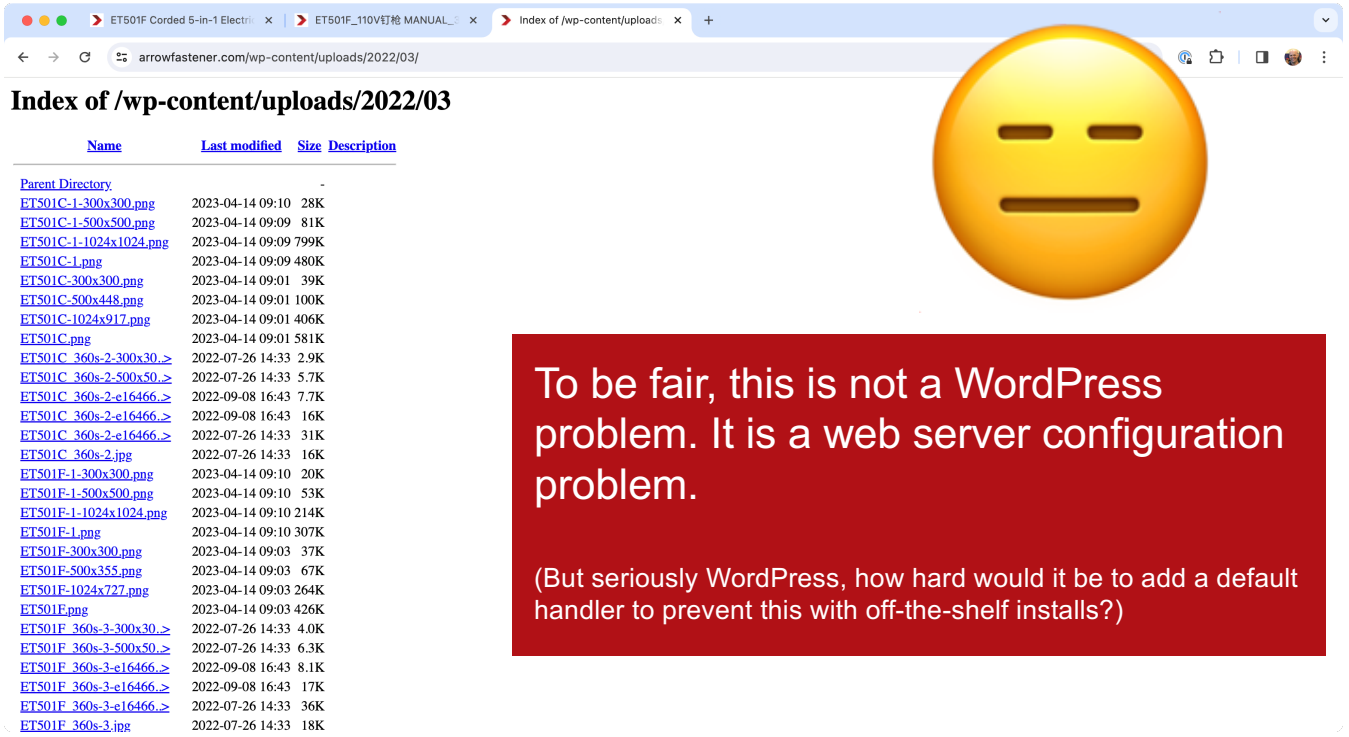


I went to find a V nail gun to make custom picture frame nailing a little easier. I have an Arrow stapler I like, so I went to the arrowfastener.com website to see if they made a product to accommodate V nails as well.

Some websites have the "WordPress look." You kinda know it's WordPress from the iconography (like the search magnifying glass), the layout, the gallery slider, and the menu orientation. But I'm really trying not to think about that right now, I'm just looking for a nail gun, like a normal person ...



... until I click to look at a product manual and now I just can't resist.

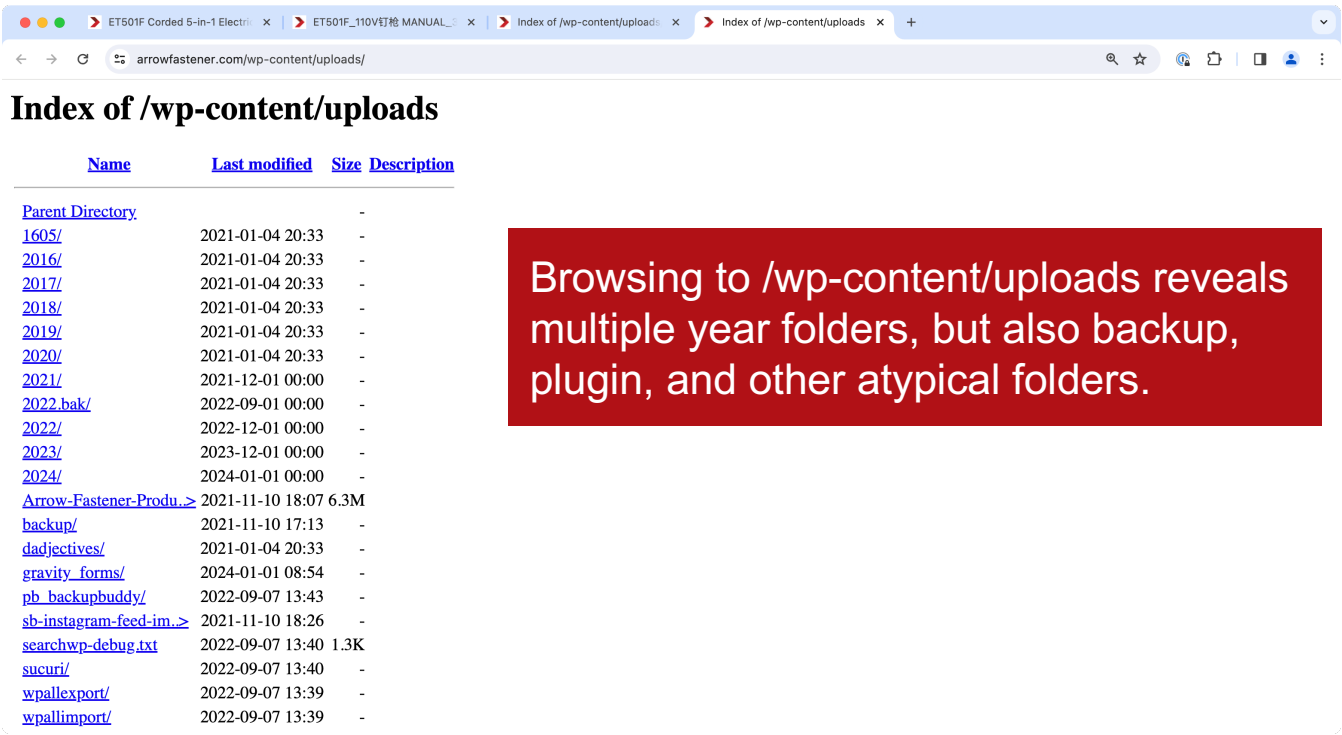


The wp-content folders on a WordPress server are a classic example of directory browsing exposure. For Arrow, it revealed mostly media file uploads for the web server, which is probably NBD.

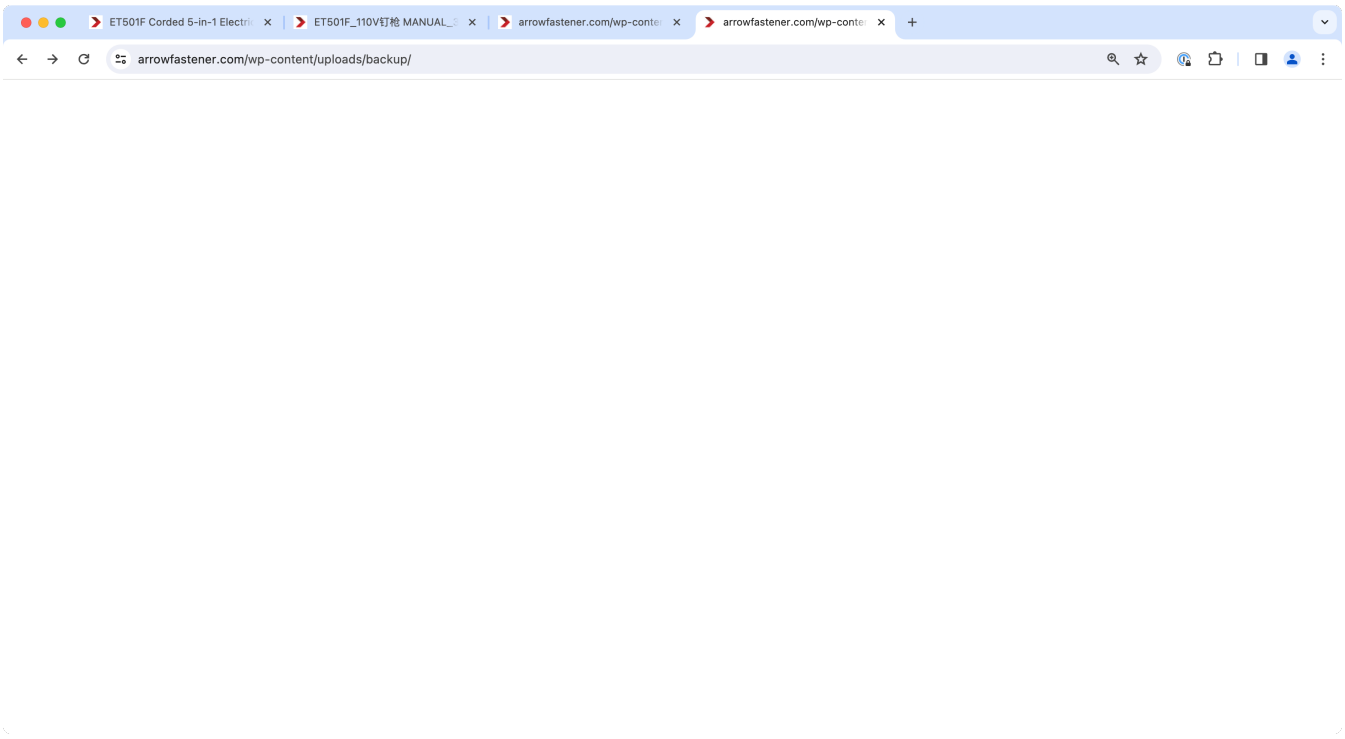
```
$ python wordpress-rest-enum.py  -w https://arrowfastener.com/ --media | jq
{
  "media": [
    "https://arrowfastener.com/wp-content/uploads/2023/06/IMG_20200227_171006.jpg",
    "https://arrowfastener.com/wp-content/uploads/2023/02/hero-30-percent-mobile.svg",
    "https://arrowfastener.com/wp-content/uploads/2023/02/hero-30-percent.svg",
    "https://arrowfastener.com/wp-content/uploads/2022/12/zoro-logo-online-retailer.jpg",
    "https://arrowfastener.com/wp-content/uploads/2022/12/Arrow_Q4Giveaway-36.jpg",
    "https://arrowfastener.com/wp-content/uploads/2022/11/oscillating-blades-
planogram_information-2022-canada.pdf",
    "https://arrowfastener.com/wp-content/uploads/2022/10/oscillating-blades-item-set-up-
sheet-2022-CANADA.pdf",
...
    "https://arrowfastener.com/wp-content/uploads/2017/12/wall-mounted-chrstms-tree-arrow-
project-hero.jpg"
  ]
}
```

Special thanks to Chris Dale @ChrisADale for automating enumeration using the WordPress API interface: https://github.com/rivsec/wordpress-rest-enum

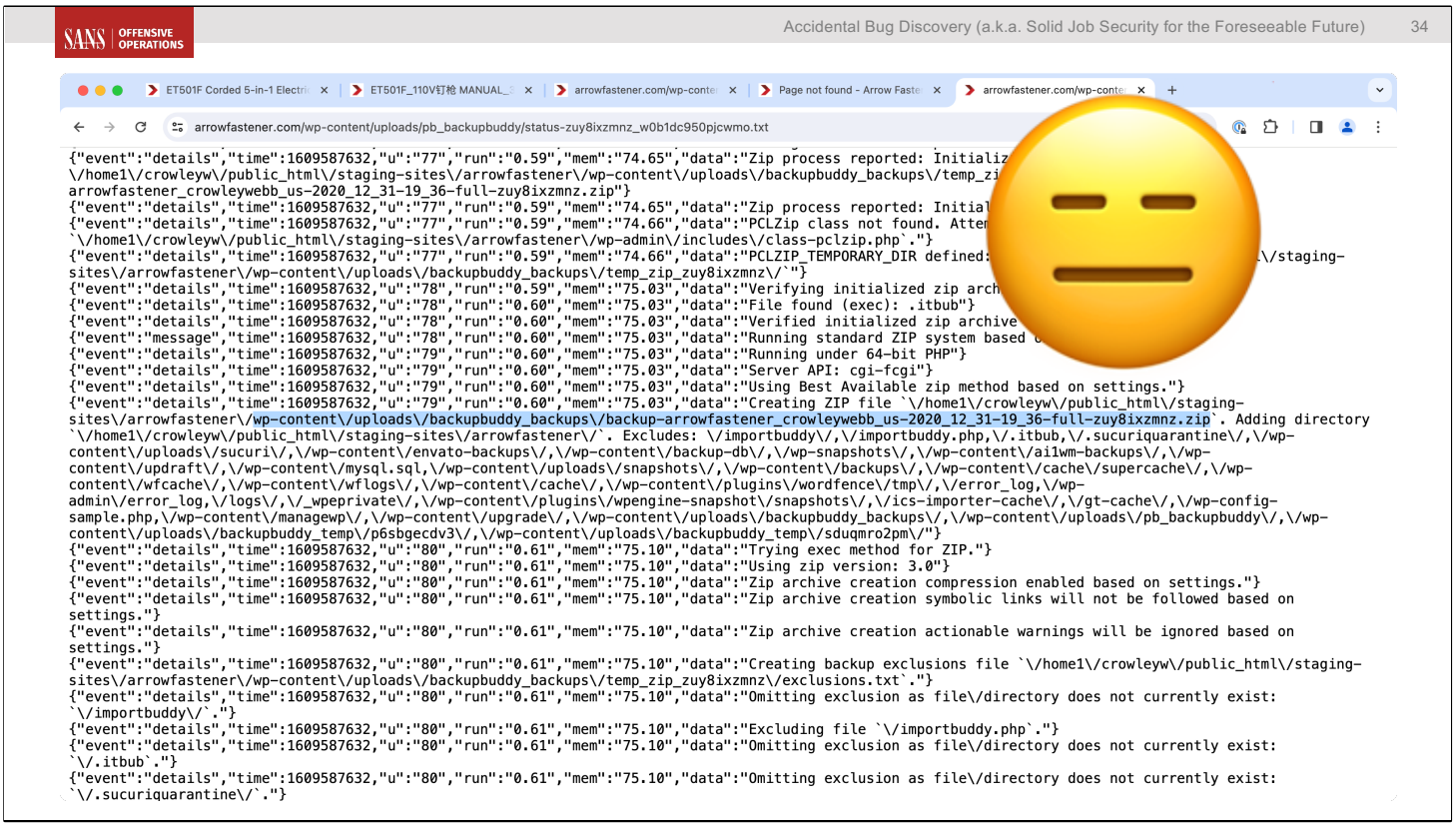
A fun tool I've learned about recently from Chris Dale (@ChrisADale) is wordpress-rest-enum that uses the WordPress API to enumerate media files, users, posts, pages, and comments from a WordPress server. The response data is returned as JSON, which makes searching the available files much easier. (This is also useful when directory browsing is disabled on the web server.)



Browsing to /wp-content/uploads revealed more than the typical media file folders though, including several backup and plugin folders.



While some folders have empty index files, returning a blank page instead of a file list (like this backup folder)...

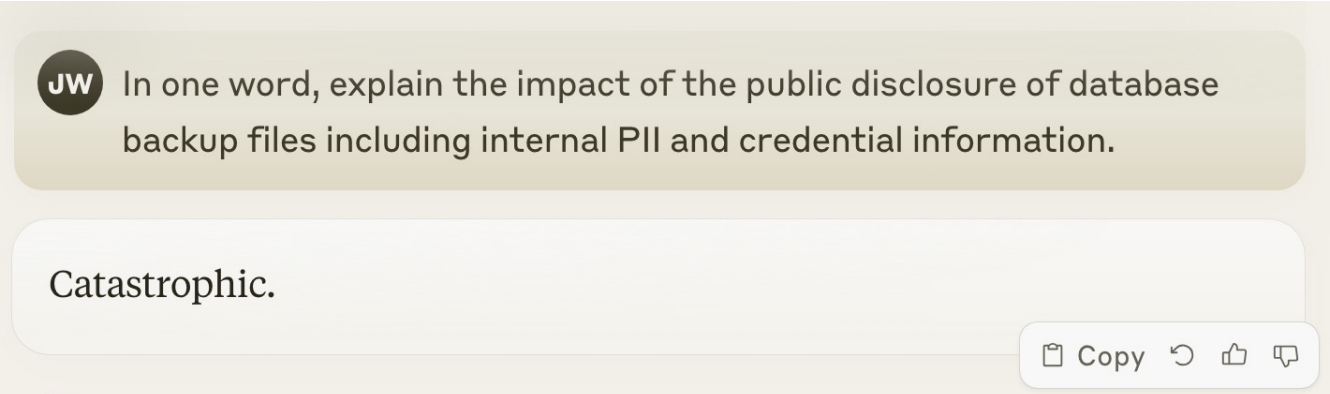


... other folders do not, like this pb_backupbuddy plugin, revealing detailed file system paths that are accessible through the web server.

Arrow Fastener Risk Assessment

- WordPress gets a lot of criticism, but the core platform has been strong for many years (plugins and themes are what ruins WordPress security)
- Arrow's site lacks web server security – you can't build strength from a shaky foundation

We love to talk about new tools, but a lot of the time just the browser itself is enough to identify critical vulnerabilities.


JW
In one word, explain the impact of the public disclosure of database backup files including internal PII and credential information.
Catastrophic.
Copy

In Review

- There's lots of bugs out there just waiting to be exploited
- Early vulnerabilities can be useful predictors of later problems
- Risk is assessed best when integrating business understanding
- Often you only need your browser for exploitation

Cyber has ruined my ability to use websites like a normal person.
I wouldn't have it any other way.

SANS | OFFENSIVE OPERATIONS

SANS SEC504: Hacker Tools, Techniques, and Incident Handling
www.sans.org/sec504

Questions?

AUTHOR

Joshua Wright

jwright@willhackforsushi.com

@joswr1ght

PEN TESTING RESOURCES

pen-testing.sans.org

@SANSPenTest