

Accidental Bug Discovery

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

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

@ 2024 JOSHUA WRIGHT | JWRIGHT@WILLHACKFORSUSHI.COM | ALL RIGHTS RESERVED

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.

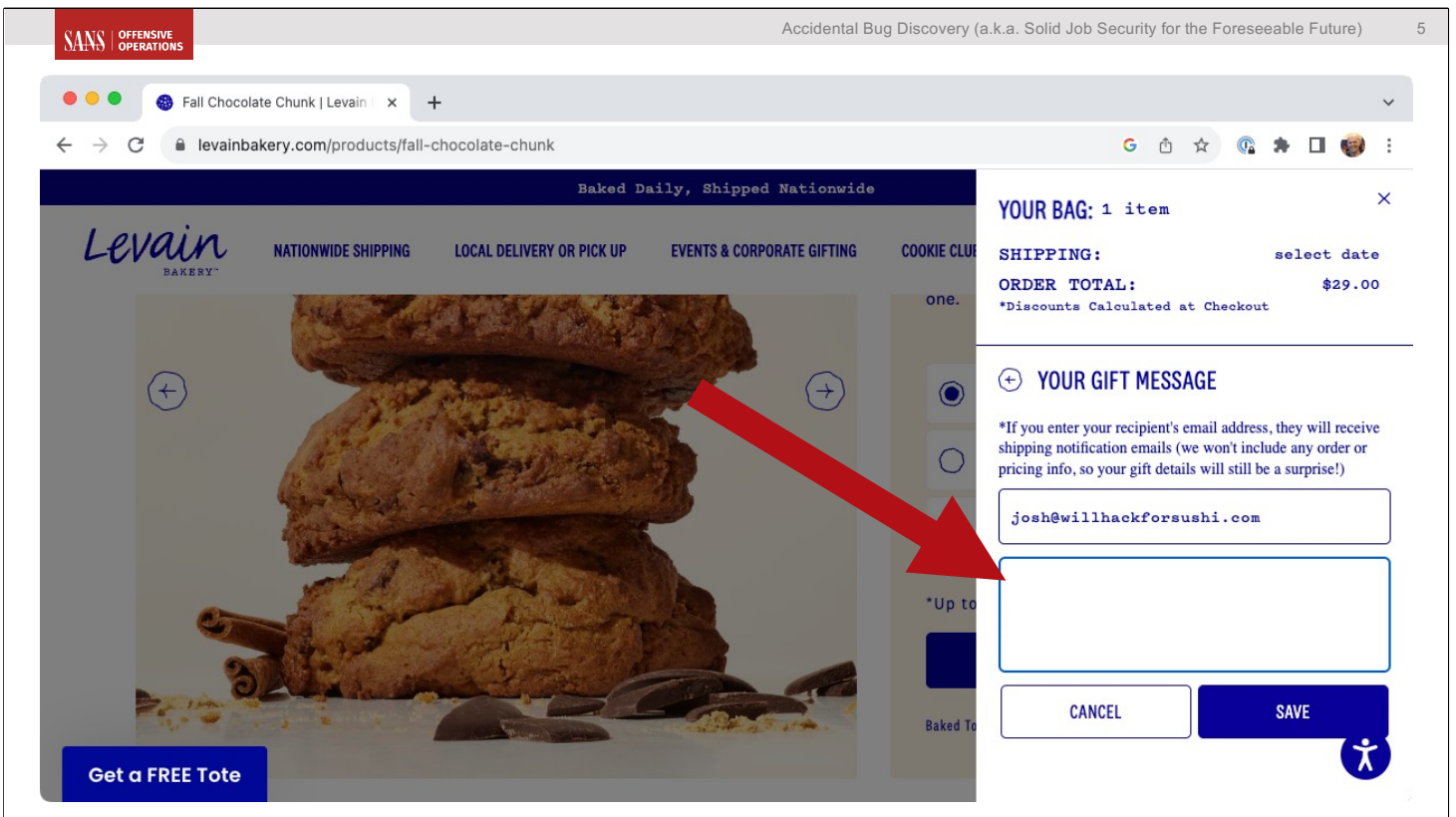


Sending Cookies as a Christmas Gift

The screenshot shows the Levain Bakery website. The browser address bar displays "Levain Bakery™ | New York City" and "levainbakery.com". The website header features the Levain Bakery logo and navigation links: "NATIONWIDE SHIPPING", "LOCAL DELIVERY OR PICK UP", "EVENTS & CORPORATE GIFTING", "COOKIE CLUB", "OUR STORY", and "OUR BAKERIES". A dark blue banner reads "Baked Daily, Shipped Nationwide".

The main content area is divided into three sections:

- COOKIE GIFT BOXES:** Features an image of a blue gift box with a white circular label that says "Here for the season: Fall Chocolate Chunk". Below the image is a button that says "ORDER NATIONWIDE SHIPPING" and a blue button that says "Get a FREE Tote".
- FAVORS & EVENTS:** Features an image of several cookies wrapped in clear plastic bags with blue ribbons. Below the image is a button that says "LEARN MORE".
- LOCAL ORDERS:** Features an image of a blue cup of coffee and a box of cookies. Below the image is a button that says "ORDER PICKUP OR DELIVERY" and a blue icon of a person with a shopping bag.



levainbakery.com says

I hope these cookies find you well! Happy Holidays! -Josh

OK

select date \$29.00

YOUR GIFT MESSAGE

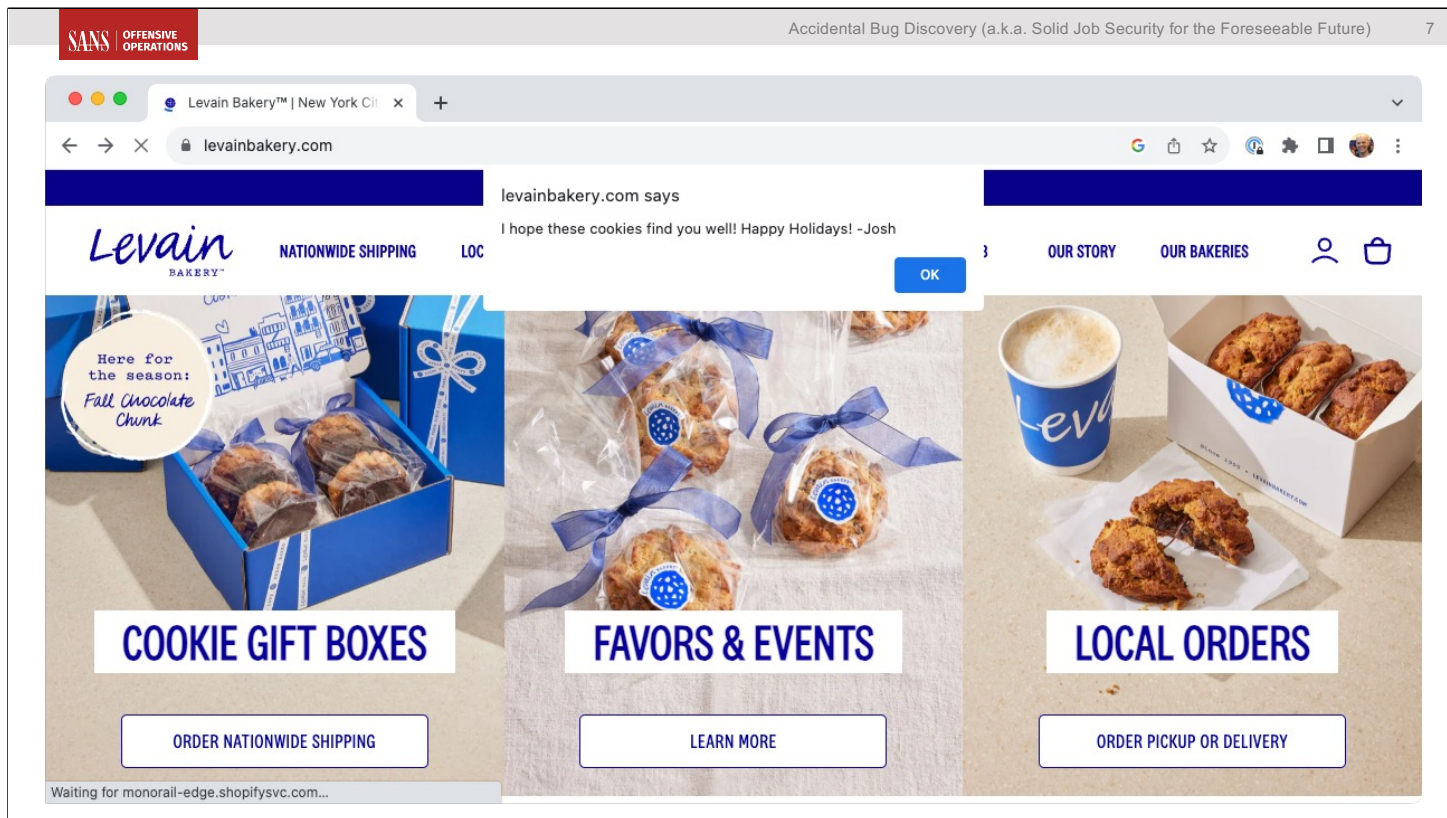
*If you enter your recipient's email address, they will receive shipping notification emails (we won't include any order or pricing info, so your gift details will still be a surprise!)

josh@willhackforsushi.com

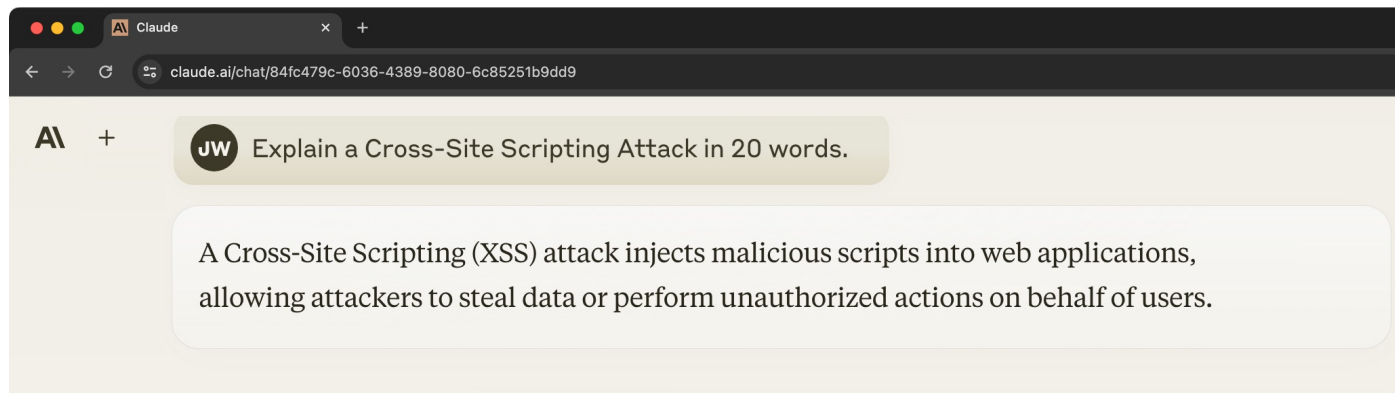
```
<script>alert('I hope these cookies find you well! Happy Holidays! - Josh')</script>
```

CANCEL SAVE

Get a FREE Tote



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



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.

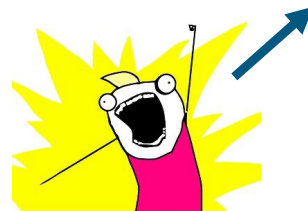
JW Limit the explanation to 1 word.

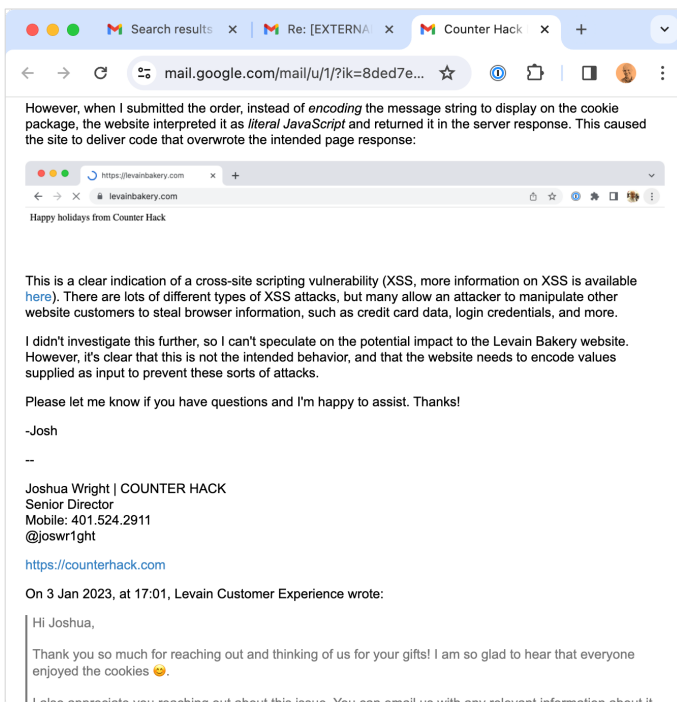
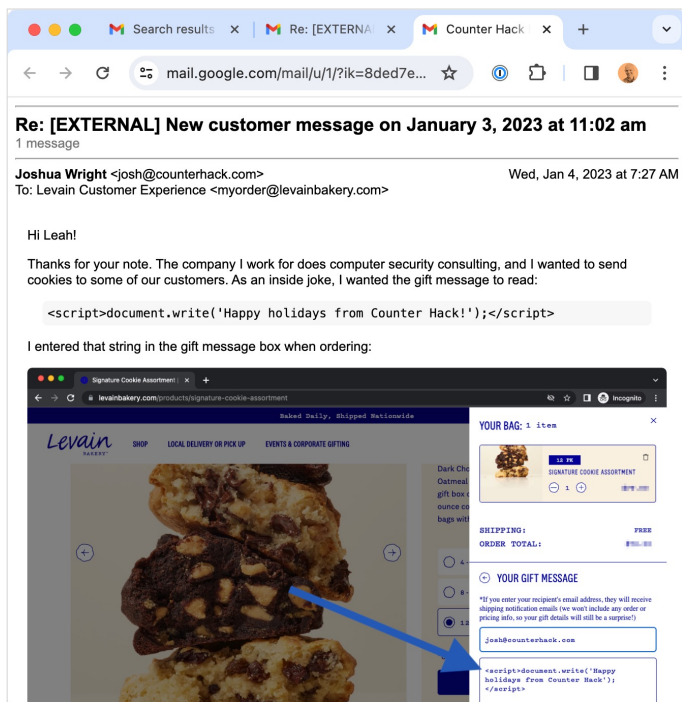
Hacksites.

Copy ↺ 👍 💬

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

Subscribe to Pro ✕



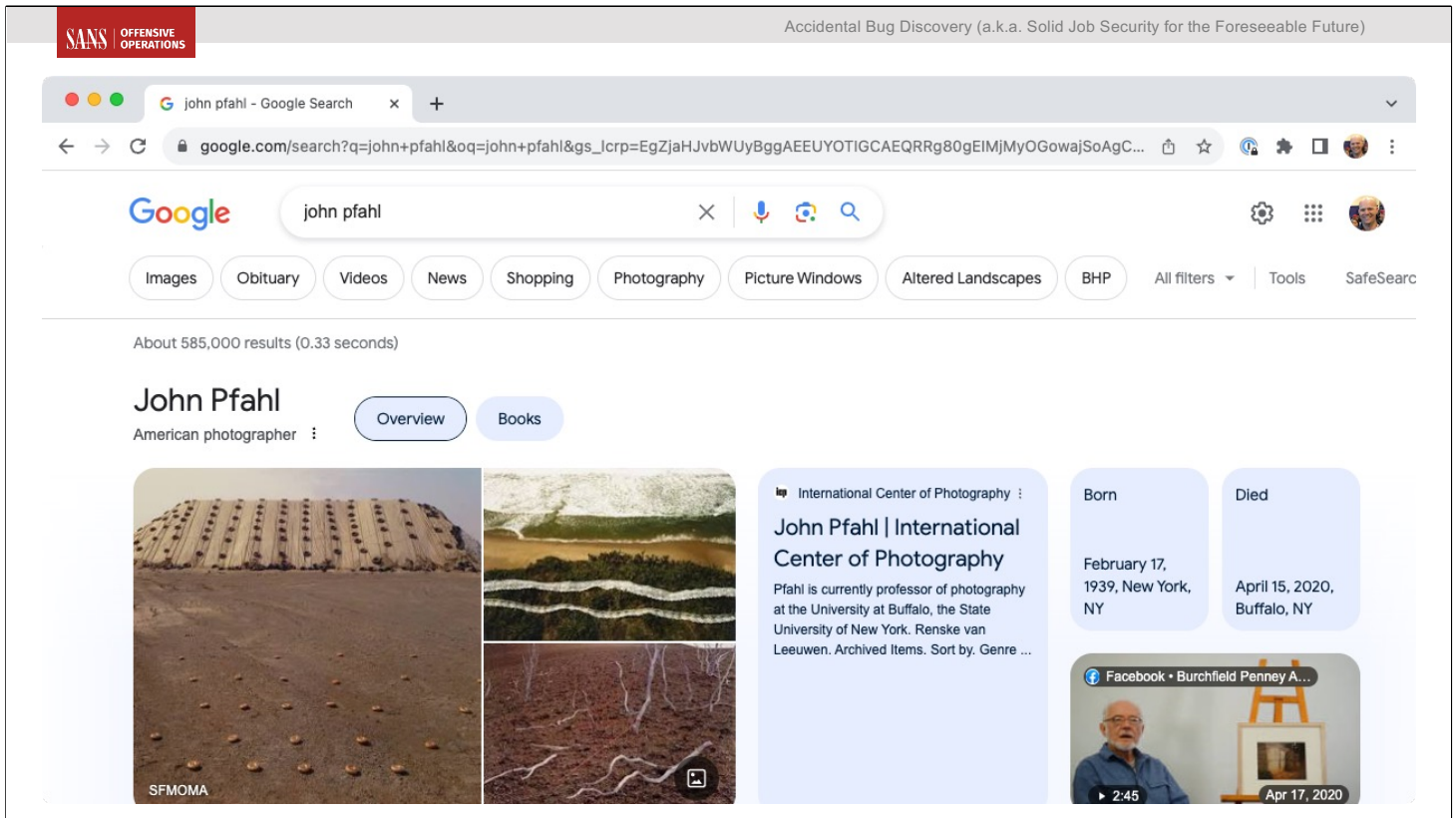


I reported the vulnerability in January 2023; still vulnerable.

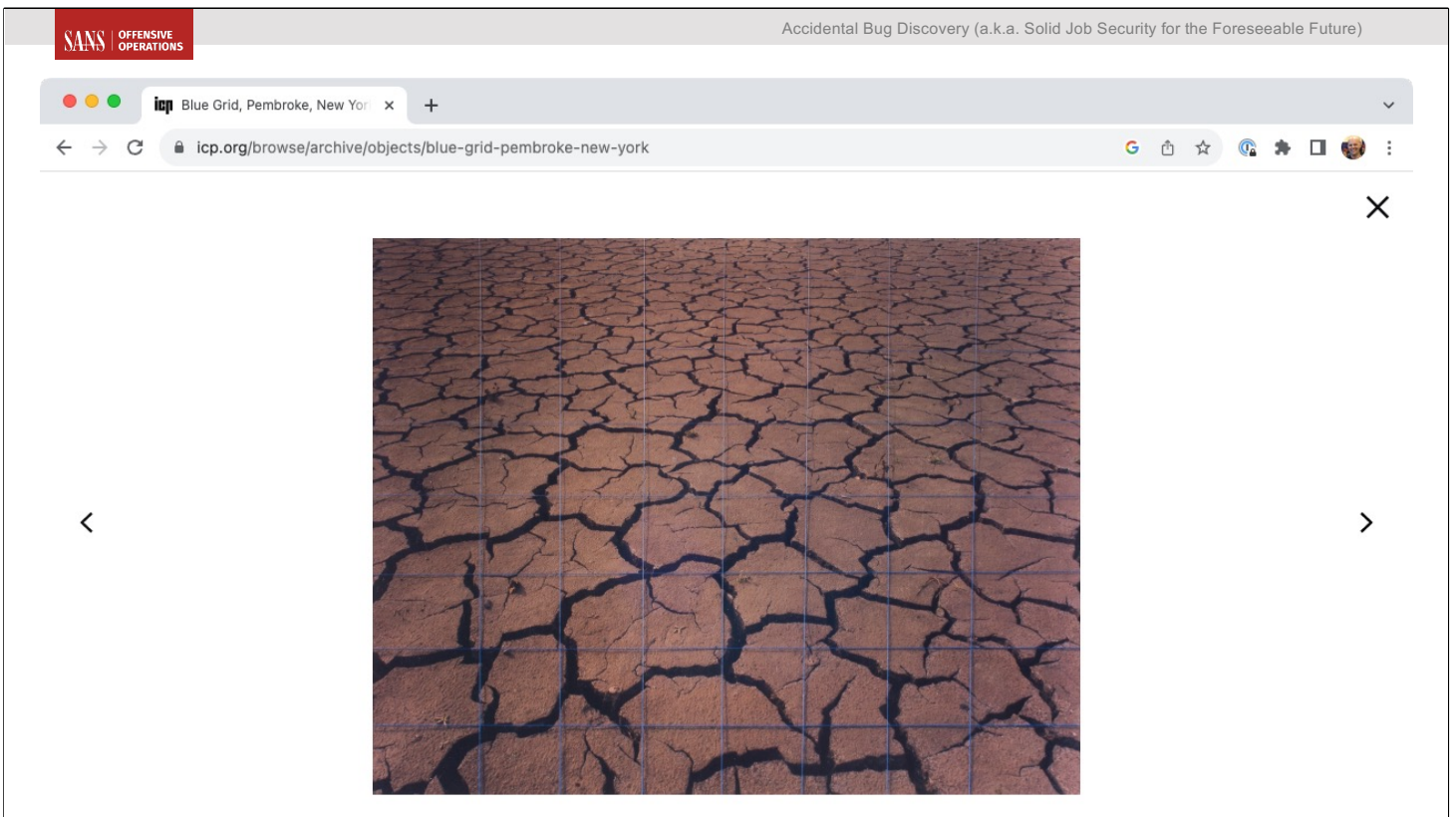
Levain Bakery Risk Assessment

- 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:

Blue Grid, Pembroke, New York

icp.org/browse/archive/objects/blue-grid-pembroke-new-york

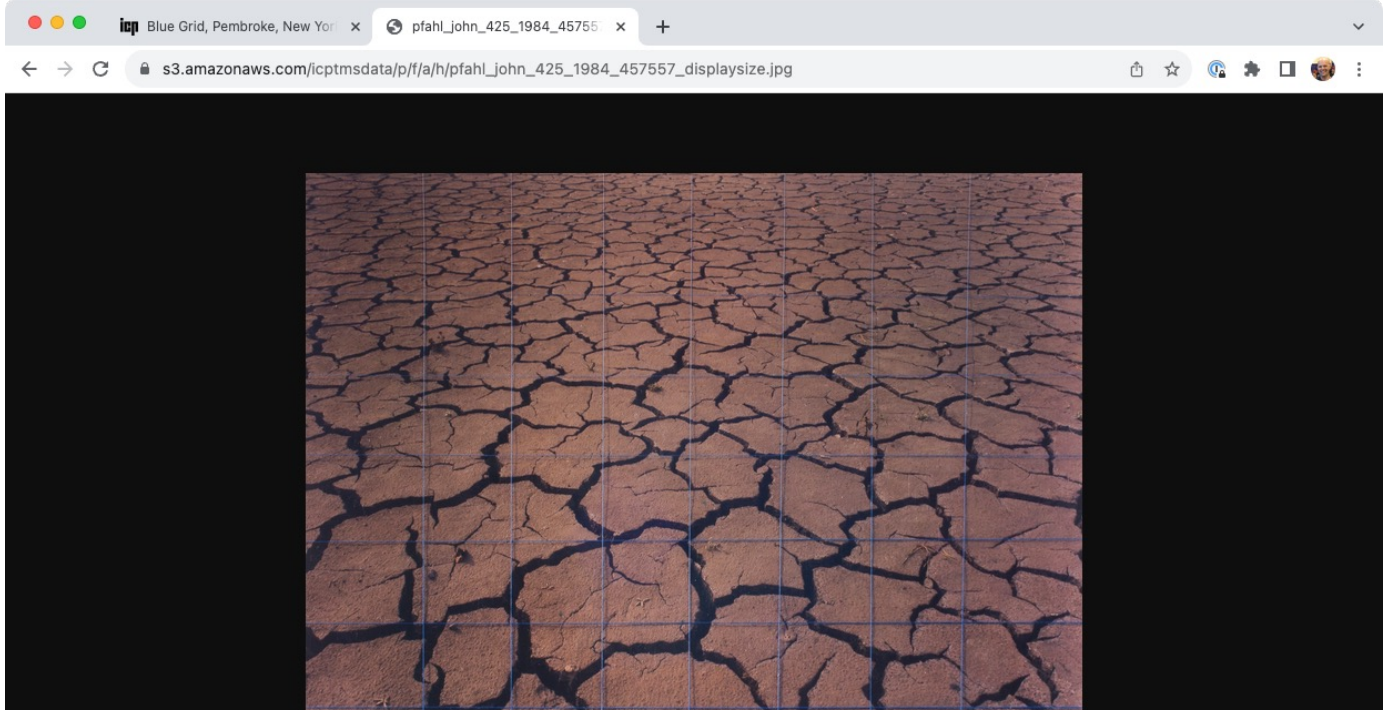
John Pfahl

Blue Grid, Pembroke, New York

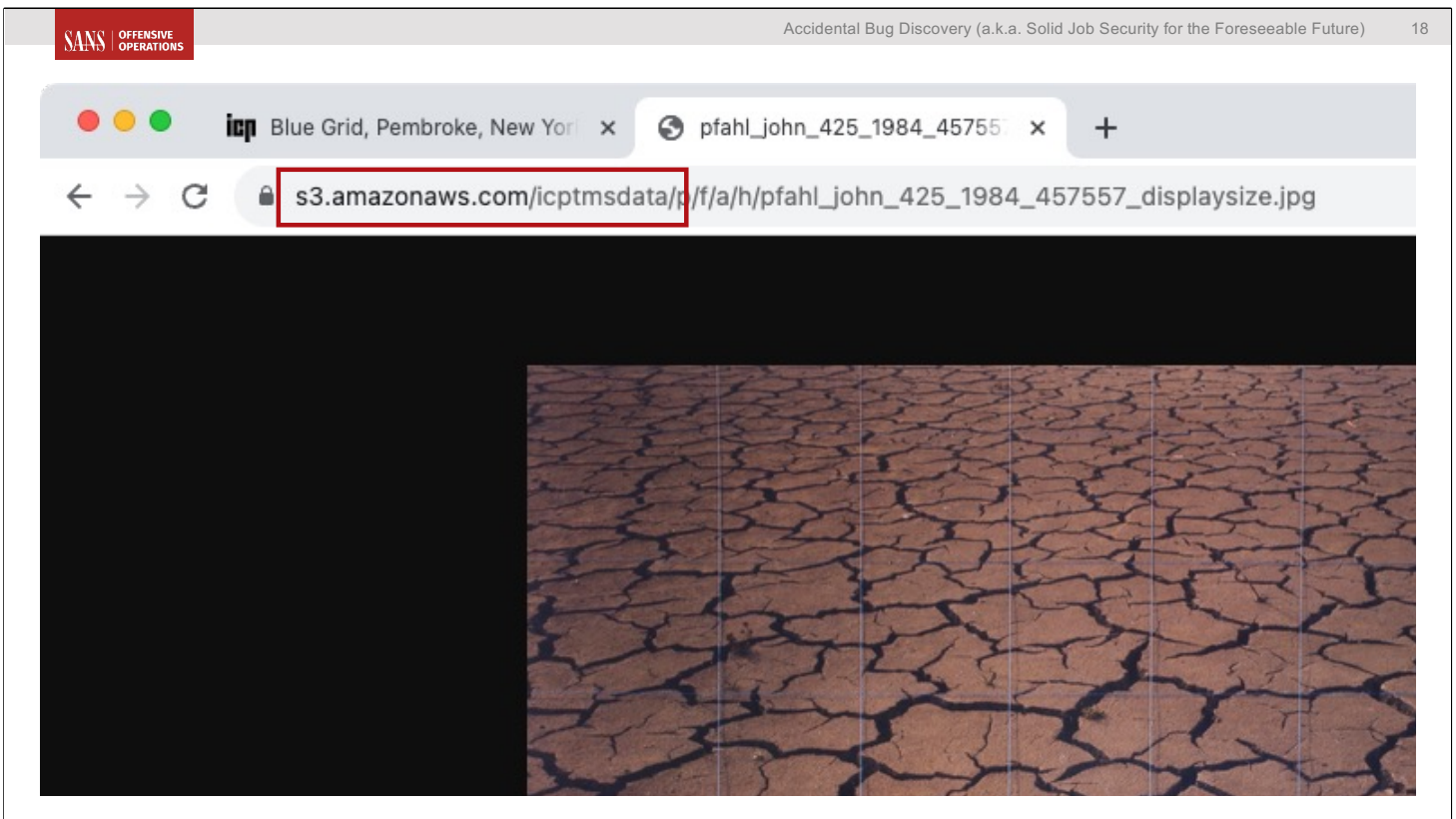


Name	Url	Type	Ini...	Waterfall
?random=1695322827...	https://googleads.g.doubleclick.net/pagead/viewthroughconversion...	script	V...	
nr-rum.b96ea0dc-1.240...	https://js-agent.newrelic.com/nr-rum.b96ea0dc-1.240.0.min.js	script	bl...	
refresh	https://marco.feathr.co/v1/refresh	gif	uti...	
form-settings?u=82f4e...	https://mc.us5.list-manage.com/subscribe/form-settings?u=82f4e3...	script	e...	
set/	https://pagead2.googleadsyndication.com/pagead/buyside_topics/set/	fetch	?r...	
integrations	https://polo.feathr.co/v1/accounts/62dca9babec5b7e1deb11cb2/int...	xhr	fe...	
pixel.js?pk=feathr	https://polo.feathr.co/v1/accounts/62dca9babec5b7e1deb11cb2/int...	script	fa...	
pixel.js?pk=feathr	https://polo.feathr.co/v1/accounts/62dca9babec5b7e1deb11cb2/pl...	script	re...	
crumb?cb=169532282...	https://polo.feathr.co/v1/analytics/crumb?cb=1695322827146&a_id...	gif	re...	
crumb?cb=169532282...	https://polo.feathr.co/v1/analytics/crumb?cb=1695322827147&a_id...	gif	re...	
script.js?pk=feathr&cb...	https://polo.feathr.co/v1/analytics/match/script.js?pk=feathr&cb=16...	script	re...	
mc-validate.js	https://s3.amazonaws.com/downloads.mailchimp.com/js/mc-valida...	script	bl...	
pfahl_john_425_1984_4...	https://s3.amazonaws.com/icptmsdata/p/f/a/h/pfahl_john_425_198...	jpeg	bl...	
10910257991?random...	https://td.doubleclick.net/td/rul/10910257991?random=169532282...	document		
?id=144399669271405...	https://www.facebook.com/tr/?id=1443996692714051&ev=Microda...	text/plain	fb...	
?id=144399669271405...	https://www.facebook.com/tr/?id=1443996692714051&ev=PageVie...	text/plain	fb...	
?id=210610338958270...	https://www.facebook.com/tr/?id=2106103389582703&ev=Microda...	text/plain	fb...	
?id=210610338958270...	https://www.facebook.com/tr/?id=2106103389582703&ev=ViewCo...	text/plain	fb...	
?id=210610338958270...	https://www.facebook.com/tr/?id=2106103389582703&ev=ViewCo...	text/plain	fb...	

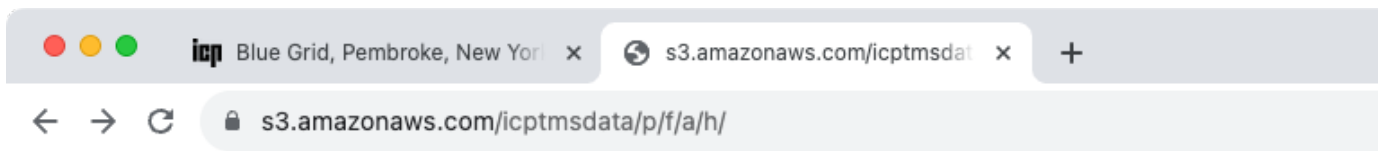
Opening developer tools, clicking the Network tab, and refreshing the page shows all the retrieved resources, including the image I want to see. From here I can open just the image in full screen.



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



Well, now I need to investigate this S3 bucket.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>NoSuchKey</Code>
  <Message>The specified key does not exist.</Message>
  <Key>p/f/a/h/</Key>
  <RequestId>2JYG2N69HNKFQ26V</RequestId>
  <HostId>q33ZgQtG369HalgPNW8b4Ir2H13tw/n02AbDmam9UzKhLDPi+kqqpeKQGlXhH4/YPMc7AMuc6nc=</HostId>
</Error>
```

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.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>icptmsdata</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>true</IsTruncated>
  <Contents>
    <Key>/a/r/t/(art)n_192_2003_435061_displaysize.jpg</Key>
    <LastModified>2018-07-24T08:47:11.000Z</LastModified>
    <ETag>"bce08ad8a3e912fa4f28e1e60b50bf9c"</ETag>
    <Size>176178</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>/a/r/t/(art)n_192_2003_435061_fullscreen.jpg</Key>
    <LastModified>2018-07-24T08:47:11.000Z</LastModified>
    <ETag>"e33bb5945d19719878c36c8eb2f68a3d"</ETag>
    <Size>744182</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>/a/r/t/(art)n_192_2003_435061_thumbnail.jpg</Key>
    <LastModified>2018-07-24T08:47:11.000Z</LastModified>
    <ETag>"58a237995a20242342a69dd1480eab2f"</ETag>
    <Size>77288</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

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.

```
{
  "Id": "icptmsdata-s3-policy",
  "Statement": [
    {
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Resource": [
        "arn:aws:s3:::icptmsdata/*"
      ],
      "Sid": "ListAndReadAccess"
    }
  ]
}
```

Grant all s3:Get* and
s3:List* actions

Apply to icptmsdata bucket
resource

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.

Setting permissions for website

docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteAccessPermissionsReqd.html

aws Search in this guide Contact Us English Return to the Console

AWS > Documentation > Amazon Simple Storage Service (S3) > User Guide

Feedback Preferences

1. Under **Buckets**, choose the name of your bucket.
2. Choose **Permissions**.
3. Under **Bucket Policy**, choose **Edit**.
4. To grant public read access for your website, copy the following bucket policy, and paste it in the **Bucket policy editor**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::Bucket-Name/*"
      ]
    }
  ]
}
```

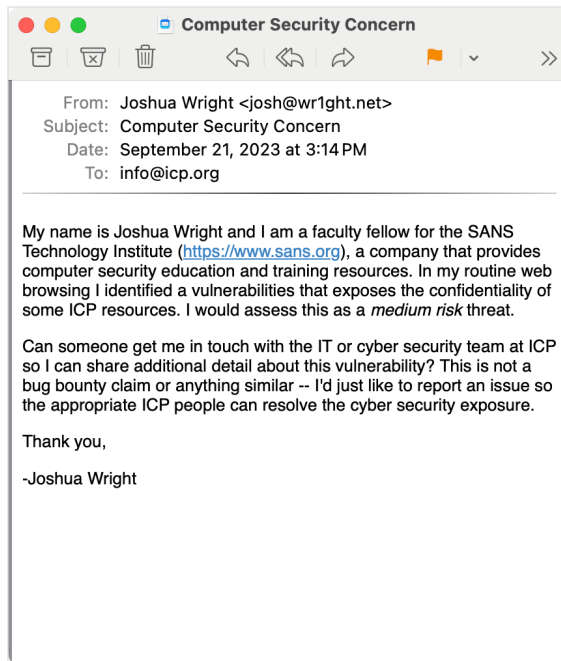
For web hosting S3 buckets, you should not grant s3:List* privileges.

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*

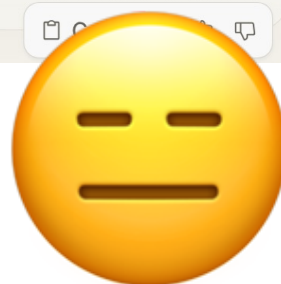
Risk assessment often requires understanding the business. A photographer who sends their original resolution pieces to ICP will likely be displeased with this vulnerability, allowing anyone to download and reproduce high-quality prints.

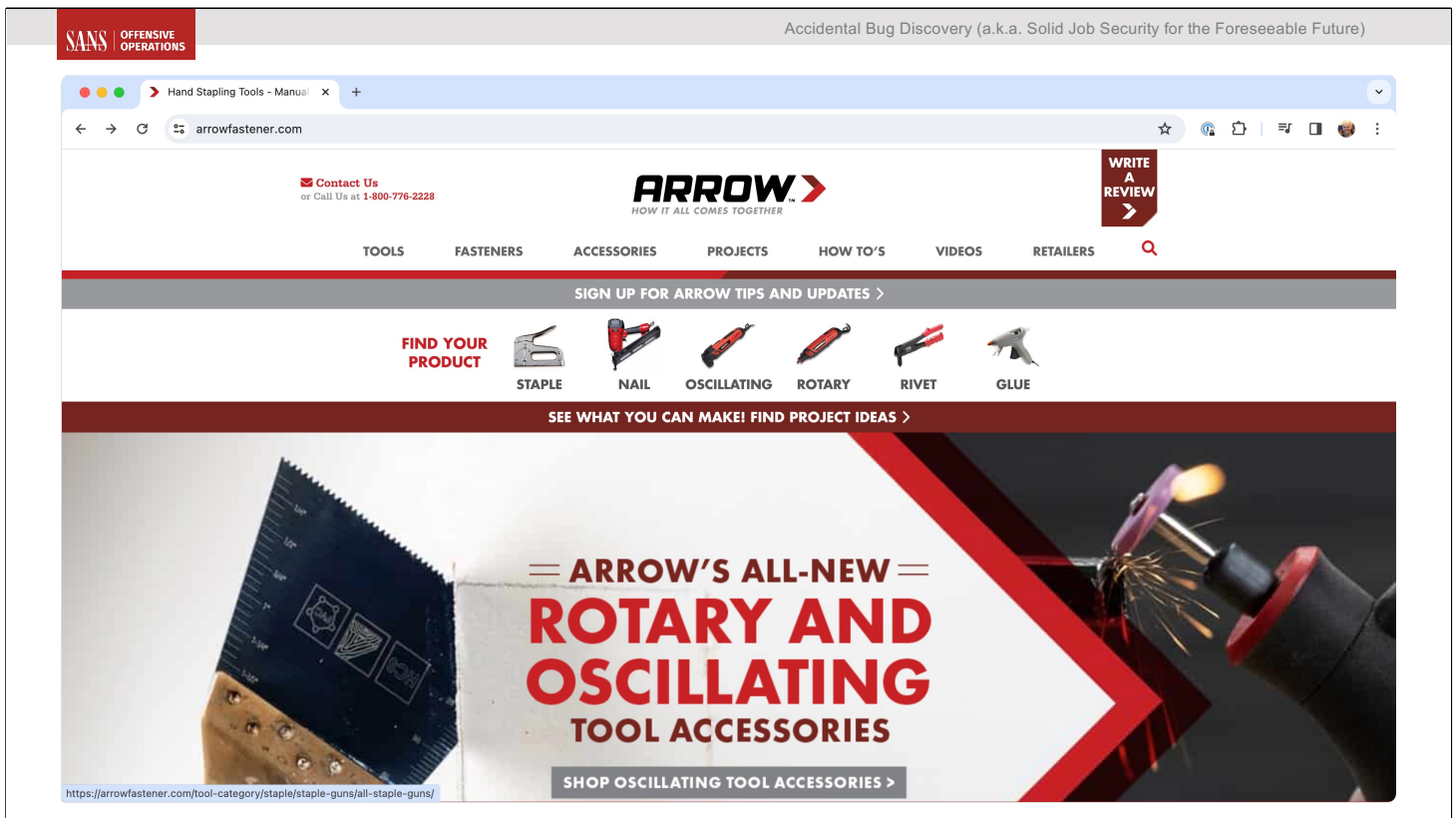


I've tried to report this vulnerability to ICP since September. No response.

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

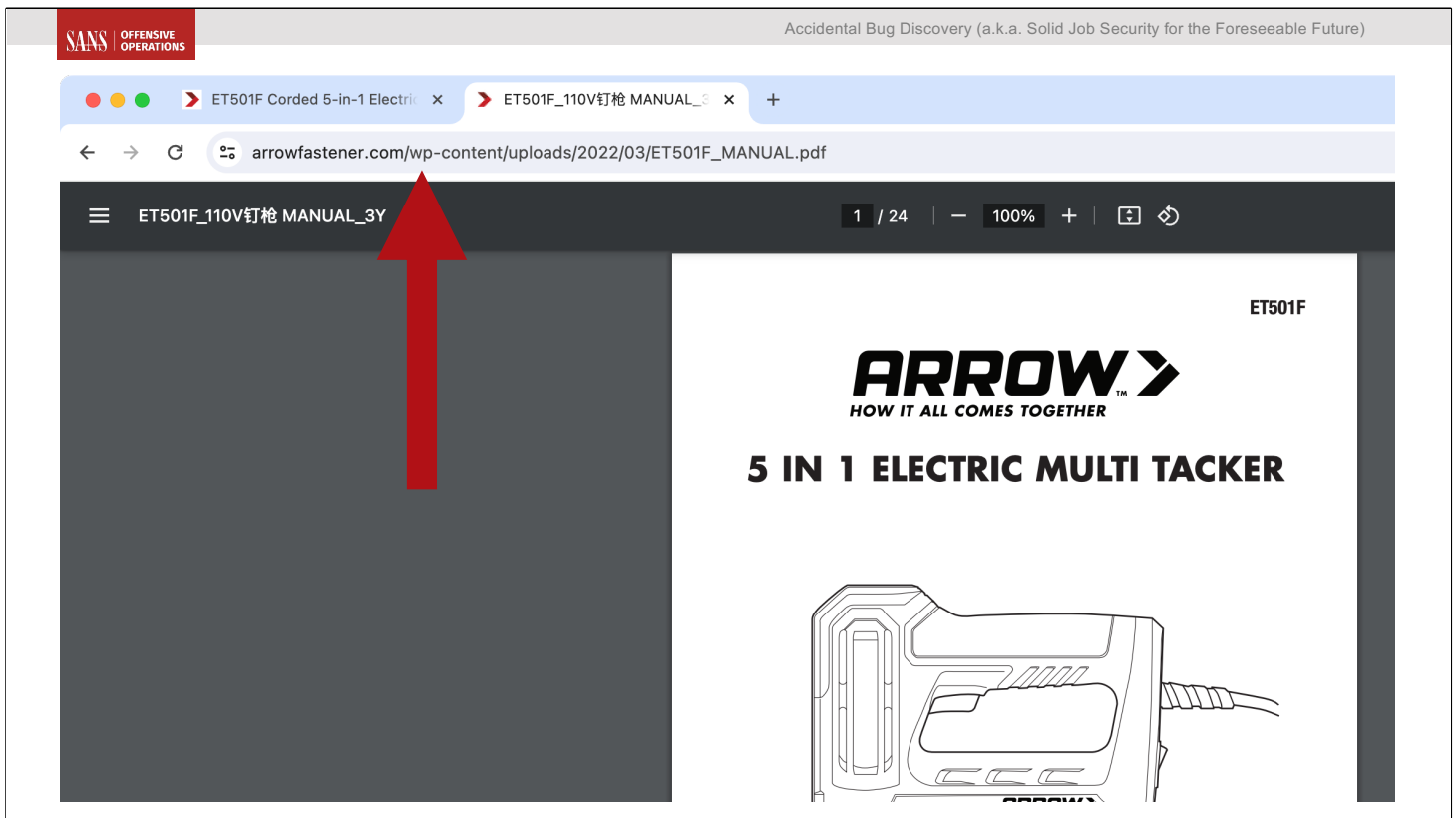
Devastating.





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 ...



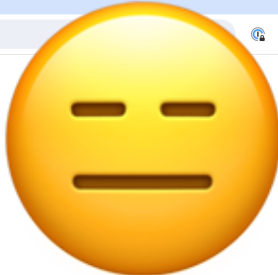
... until I click to look at a product manual and now I just can't resist.

ET501F Corded 5-in-1 Electric... x ET501F_110V钉枪 MANUAL... x Index of /wp-content/uploads/... x

arrowfastener.com/wp-content/uploads/2022/03/

Index of /wp-content/uploads/2022/03

Name	Last modified	Size	Description
Parent Directory	-	-	-
ET501C-1-300x300.png	2023-04-14 09:10	28K	
ET501C-1-500x500.png	2023-04-14 09:09	81K	
ET501C-1-1024x1024.png	2023-04-14 09:09	799K	
ET501C-1.png	2023-04-14 09:09	480K	
ET501C-300x300.png	2023-04-14 09:01	39K	
ET501C-500x448.png	2023-04-14 09:01	100K	
ET501C-1024x917.png	2023-04-14 09:01	406K	
ET501C.png	2023-04-14 09:01	581K	
ET501C_360s-2-300x30->	2022-07-26 14:33	2.9K	
ET501C_360s-2-500x50->	2022-07-26 14:33	5.7K	
ET501C_360s-2-e16466->	2022-09-08 16:43	7.7K	
ET501C_360s-2-e16466->	2022-09-08 16:43	16K	
ET501C_360s-2-e16466->	2022-07-26 14:33	31K	
ET501C_360s-2.jpg	2022-07-26 14:33	16K	
ET501F-1-300x300.png	2023-04-14 09:10	20K	
ET501F-1-500x500.png	2023-04-14 09:10	53K	
ET501F-1-1024x1024.png	2023-04-14 09:10	214K	
ET501F-1.png	2023-04-14 09:10	307K	
ET501F-300x300.png	2023-04-14 09:03	37K	
ET501F-500x355.png	2023-04-14 09:03	67K	
ET501F-1024x727.png	2023-04-14 09:03	264K	
ET501F.png	2023-04-14 09:03	426K	
ET501F_360s-3-300x30->	2022-07-26 14:33	4.0K	
ET501F_360s-3-500x50->	2022-07-26 14:33	6.3K	
ET501F_360s-3-e16466->	2022-09-08 16:43	8.1K	
ET501F_360s-3-e16466->	2022-09-08 16:43	17K	
ET501F_360s-3-e16466->	2022-07-26 14:33	36K	
ET501F_360s-3.jpg	2022-07-26 14:33	18K	



To be fair, this is not a WordPress problem. It is a web server configuration problem.

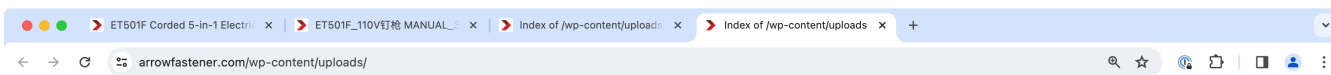
(But seriously WordPress, how hard would it be to add a default handler to prevent this with off-the-shelf installs?)

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.)

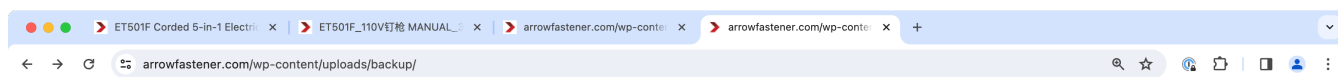


Index of /wp-content/uploads

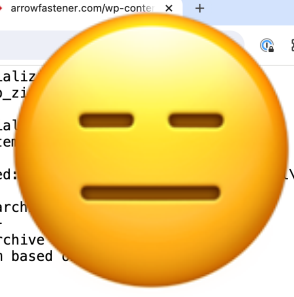
Name	Last modified	Size	Description
Parent Directory	-	-	-
1605/	2021-01-04 20:33	-	-
2016/	2021-01-04 20:33	-	-
2017/	2021-01-04 20:33	-	-
2018/	2021-01-04 20:33	-	-
2019/	2021-01-04 20:33	-	-
2020/	2021-01-04 20:33	-	-
2021/	2021-12-01 00:00	-	-
2022.bak/	2022-09-01 00:00	-	-
2022/	2022-12-01 00:00	-	-
2023/	2023-12-01 00:00	-	-
2024/	2024-01-01 00:00	-	-
Arrow-Fastener-Produ.>	2021-11-10 18:07	6.3M	-
backup/	2021-11-10 17:13	-	-
dadjectives/	2021-01-04 20:33	-	-
gravity_forms/	2024-01-01 08:54	-	-
pb_backupbuddy/	2022-09-07 13:43	-	-
sb-instagram-feed-im.>	2021-11-10 18:26	-	-
searchwp-debug.txt	2022-09-07 13:40	1.3K	-
sucuri/	2022-09-07 13:40	-	-
wpallexport/	2022-09-07 13:39	-	-
wpallimport/	2022-09-07 13:39	-	-

Browsing to /wp-content/uploads reveals multiple year folders, but also backup, plugin, and other atypical folders.

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)...



```
ET501F Corded 5-in-1 Electric Drill - 10000mAh Lithium-Ion Battery Pack - 2020-12-31-19-36-full-zuy8ixzmnz.zip
ET501F_110V电钻 MANUAL - 10000mAh Lithium-Ion Battery Pack - 2020-12-31-19-36-full-zuy8ixzmnz.zip
arrowfastener.com/wp-content/uploads/pb_backupbuddy/status-zuy8ixzmnz_w0b1dc950pjcwmo.txt
Page not found - Arrow Fastener
arrowfastener.com/wp-content/uploads/pb_backupbuddy/status-zuy8ixzmnz_w0b1dc950pjcwmo.txt

{"event": "details", "time": 1609587632, "u": "77", "run": "0.59", "mem": "74.65", "data": "Zip process reported: Initializ
/home1/crowleyw/public_html/staging-sites/arrowfastener/wp-content/uploads/backupbuddy_backups/temp_zi
arrowfastener_crowleywebb_us-2020_12_31-19_36-full-zuy8ixzmnz.zip"}
{"event": "details", "time": 1609587632, "u": "77", "run": "0.59", "mem": "74.65", "data": "Zip process reported: Initial
arrowfastener_crowleywebb_us-2020_12_31-19_36-full-zuy8ixzmnz.zip"}
{"event": "details", "time": 1609587632, "u": "77", "run": "0.59", "mem": "74.66", "data": "PCLZip class not found. Atter
/home1/crowleyw/public_html/staging-sites/arrowfastener/wp-admin/includes/class-pclzip.php."}
{"event": "details", "time": 1609587632, "u": "77", "run": "0.59", "mem": "74.66", "data": "PCLZIP_TEMPORARY_DIR defined:
/sites/arrowfastener/wp-content/uploads/backupbuddy_backups/temp_zip_zuy8ixzmnz/"
{"event": "details", "time": 1609587632, "u": "78", "run": "0.59", "mem": "75.03", "data": "Verifying initialized zip arch
{"event": "details", "time": 1609587632, "u": "78", "run": "0.60", "mem": "75.03", "data": "File found (exec): .itbub"}
{"event": "details", "time": 1609587632, "u": "78", "run": "0.60", "mem": "75.03", "data": "Verified initialized zip archive
{"event": "message", "time": 1609587632, "u": "78", "run": "0.60", "mem": "75.03", "data": "Running standard ZIP system based
{"event": "details", "time": 1609587632, "u": "78", "run": "0.60", "mem": "75.03", "data": "Running under 64-bit PHP"}
{"event": "details", "time": 1609587632, "u": "79", "run": "0.60", "mem": "75.03", "data": "Server API: cgi-fcgi"}
{"event": "details", "time": 1609587632, "u": "79", "run": "0.60", "mem": "75.03", "data": "Using Best Available zip method based on settings."}
{"event": "details", "time": 1609587632, "u": "79", "run": "0.60", "mem": "75.03", "data": "Creating ZIP file `\\home1\\crowleyw\\public_html\\staging-
sites\\arrowfastener\\wp-content\\uploads\\backupbuddy_backups\\backup-arrowfastener_crowleywebb_us-2020_12_31-19_36-full-zuy8ixzmnz.zip`. Adding directory
`\\home1\\crowleyw\\public_html\\staging-sites\\arrowfastener\\`. Excludes: `\\importbuddy\\`, `\\importbuddy.php`, `\\itbub`, `\\sucuriquarantine\\`, `\\wp-
content\\uploads\\sucuri\\`, `\\wp-content\\envato-backups\\`, `\\wp-content\\backup-db\\`, `\\wp-snapshots\\`, `\\wp-content\\ai1wm-backups\\`, `\\wp-
content\\updraft\\`, `\\wp-content\\mysql.sql`, `\\wp-content\\uploads\\snapshots\\`, `\\wp-content\\backups\\`, `\\wp-content\\cache\\supercache\\`, `\\wp-
content\\wfcache\\`, `\\wp-content\\wlogs\\`, `\\wp-content\\cache\\`, `\\wp-content\\plugins\\wordfence\\tmp\\`, `\\error_log`, `\\wp-
admin\\error_log`, `\\logs\\`, `\\_wpprivate\\`, `\\wp-content\\plugins\\wpengine-snapshot\\snapshots\\`, `\\ics-importer-cache\\`, `\\gt-cache\\`, `\\wp-config-
sample.php`, `\\wp-content\\managewp\\`, `\\wp-content\\upgrade\\`, `\\wp-content\\uploads\\backupbuddy_backups\\`, `\\wp-content\\uploads\\pb_backupbuddy\\`, `\\wp-
content\\uploads\\backupbuddy_temp\\p6sbgedcv3\\`, `\\wp-content\\uploads\\backupbuddy_temp\\sduqmo2pm\\`"}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Trying exec method for ZIP."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Using zip version: 3.0"}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Zip archive creation compression enabled based on settings."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Zip archive creation symbolic links will not be followed based on
settings."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Zip archive creation actionable warnings will be ignored based on
settings."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Creating backup exclusions file `\\home1\\crowleyw\\public_html\\staging-
sites\\arrowfastener\\wp-content\\uploads\\backupbuddy_backups\\temp_zip_zuy8ixzmnz\\exclusions.txt`."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Omitting exclusion as file\\directory does not currently exist:
`\\importbuddy\\`."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Excluding file `\\importbuddy.php`."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Omitting exclusion as file\\directory does not currently exist:
`\\itbub`."}
{"event": "details", "time": 1609587632, "u": "80", "run": "0.61", "mem": "75.10", "data": "Omitting exclusion as file\\directory does not currently exist:
`\\sucuriquarantine\\`."}
```

... 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.

Questions?

AUTHOR

Joshua Wright

jwright@willhackforsushi.com

[@joswr1ght](https://twitter.com/joswr1ght)

PEN TESTING RESOURCES

pen-testing.sans.org

[@SANSPenTest](https://twitter.com/SANSPenTest)