Confessions of a pentesitng punk

by woland

Disclaimer

- Images are not from actual engagements
- Attacks vectors are real, pictures are not.

Shall we play a name?

- Professional pentesting professional
- Ex-journo, phone phreak, and bartender
- I even passed a SANS exam!

What we do….?

- We are paid to hack into our targets and pwn as many things as possible in the time that is allotted to us.

What we do….?

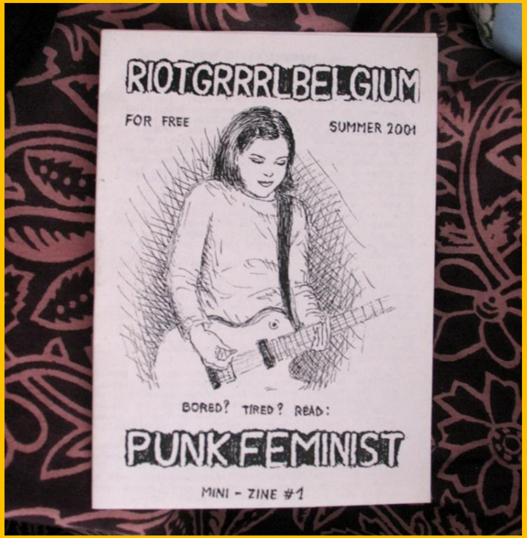
- ~~We are paid to hack into our targets and pwn as many things as possible in the time that is allotted to us.~~
- Hack into our targets
- Identify as many vulnerabilities as possible in the time allotted
- Document all findings and validate our data
- Offer an honest risk assessment and recommendations to mitigate risk
- Act ethically and with integrity when we do so

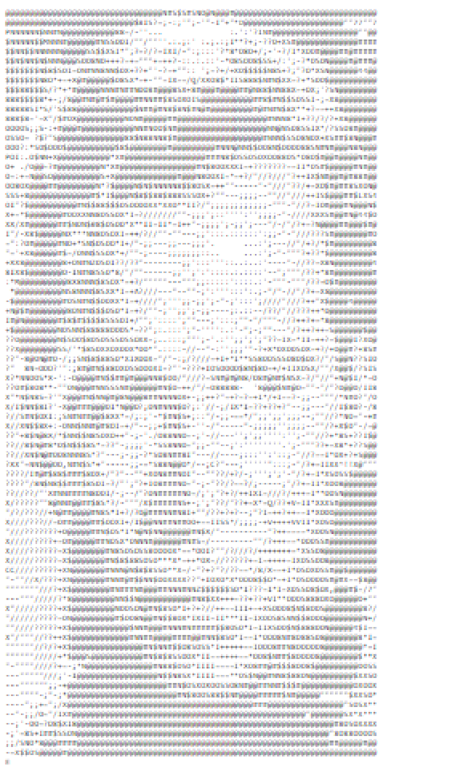
A (brief) tale of 2 subcultures

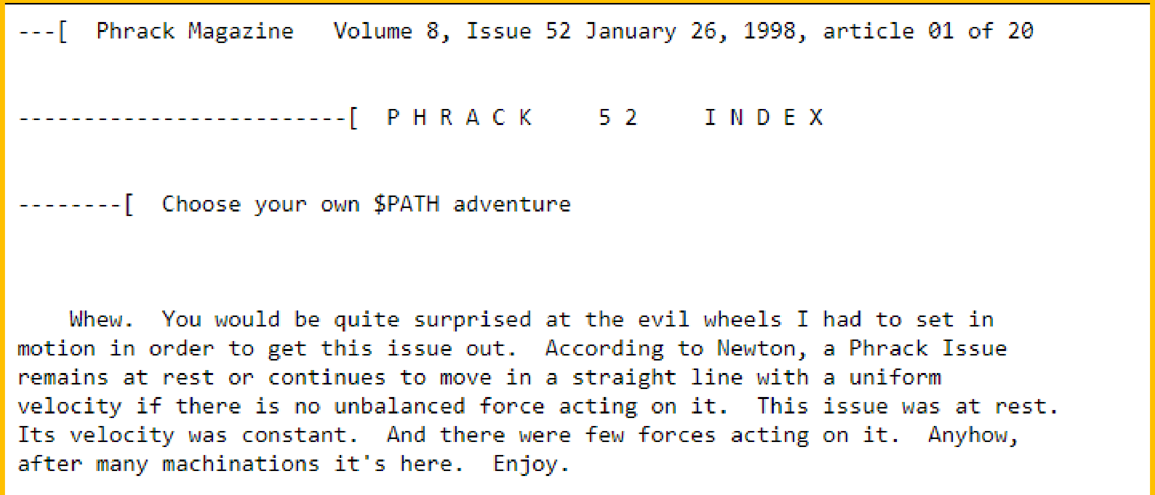
Raw Punk Streets UK 1979-1982 by Janette Beckman from Café Royal Books

Photo by Jose Chalet-Hernandez

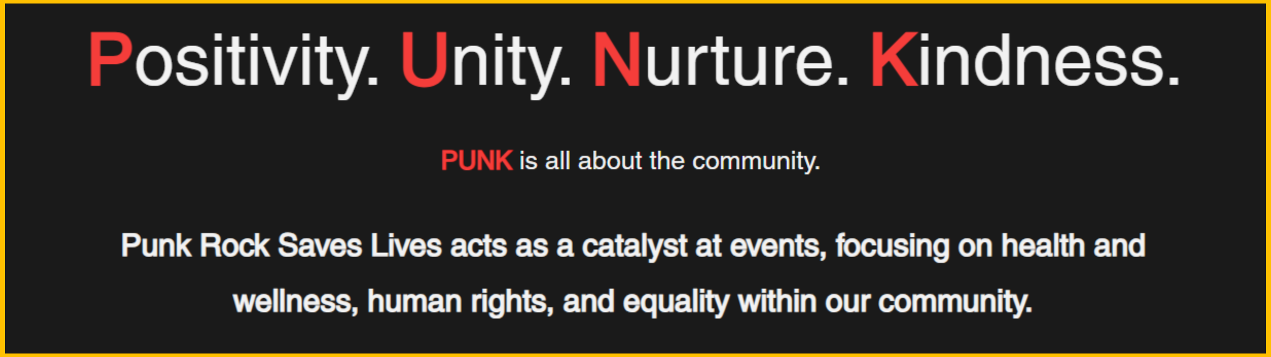
2014 © Dave Bullock Financial Times







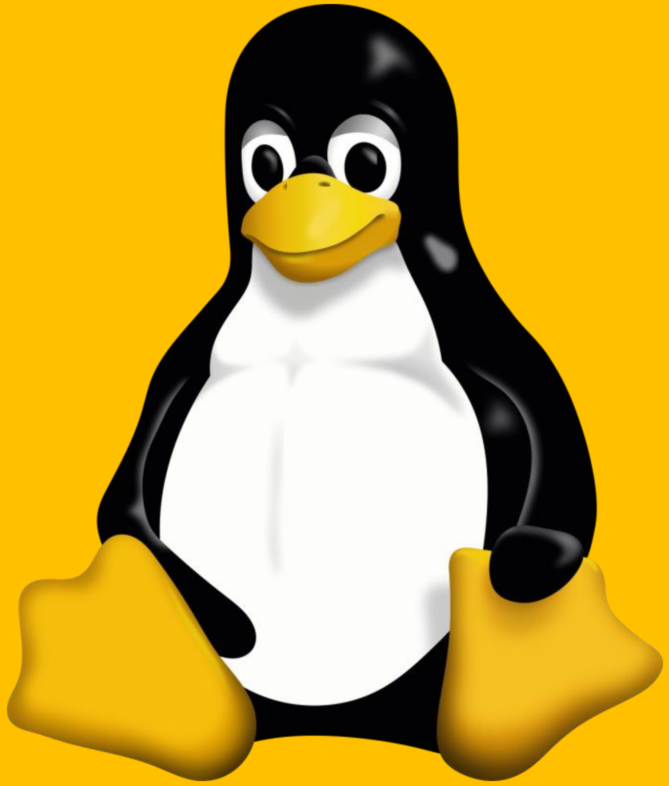
```
---[  Phrack Magazine   Volume 8, Issue 52 January 26, 1998, article 01 of 20


-------------------------[  P H R A C K     5 2     I N D E X


--------[  Choose your own $PATH adventure



    Whew.  You would be quite surprised at the evil wheels I had to set in
motion in order to get this issue out.  According to Newton, a Phrack Issue
remains at rest or continues to move in a straight line with a uniform
velocity if there is no unbalanced force acting on it.  This issue was at rest.
Its velocity was constant.  And there were few forces acting on it.  Anyhow,
after many machinations it's here.  Enjoy.
```

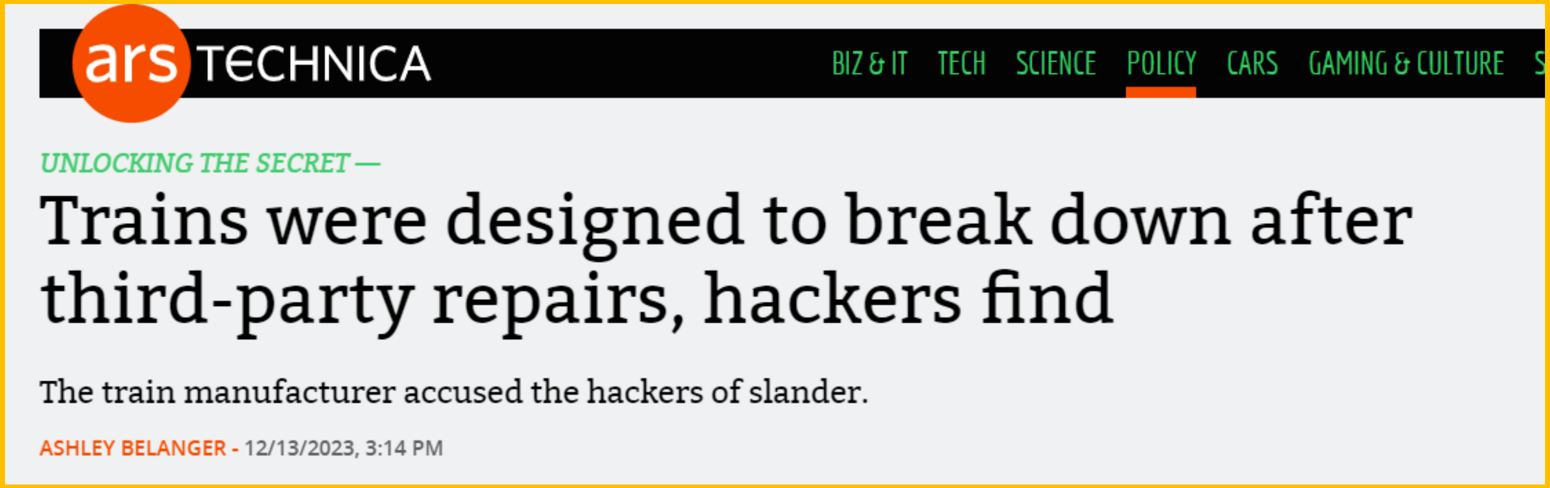


Positivity. Unity. Nurture. Kindness.

PUNK is all about the community.

Punk Rock Saves Lives acts as a catalyst at events, focusing on health and wellness, human rights, and equality within our community.



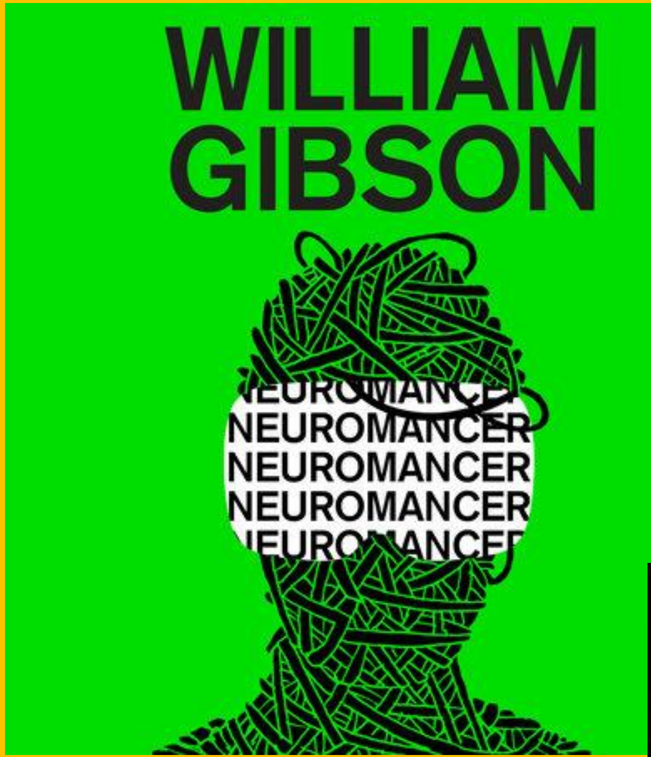


UNLOCKING THE SECRET —

Trains were designed to break down after third-party repairs, hackers find

The train manufacturer accused the hackers of slander.

ASHLEY BELANGER - 12/13/2023, 3:14 PM



WILLIAM
GIBSON

NEUROMANCER
NEUROMANCER
NEUROMANCER
NEUROMANCER
NEUROMANCER
NEUROMANCER

#1 pentesting rule of all time and forever

Written permission from an authorized party with clear definition of scope.

Protect yourself.

Different engagements

- External
- Application
- Internal
- Wireless
- Cloud
- PCI
- Phishing
- Physical
- OT/ICS
- IoT/Embedded
- Password/IAM
- Mobile
- AI

Methodologies…

- Sweet science of pentesting
- Playbook for how to test and what to hit
- But there’s a secret…
- Living document, continuously updated

DIY methodologies

- Be a punk/hacker and do it yourself
- You don’t need permission to start building your own
- Guidance + experience + time == a working methodology

Methodology guidance

- https://owasp.org/www-project-web-security-testing-guide/stable/
- https://github.com/geeksniper/active-directory-pentest
- https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet
- https://github.com/hmaverickadams/External-Pentest-Checklist
- https://github.com/J3rryBl4nks/PasswordCrackingMethodology

Report writing.. “Yay!”

- Do you like to write?

  …because there’s a lot of it
- Deadlines, and peer reviews, and QA, o my!

You can’t blow it up

- Denial of service ain’t just for packets
- My fun external testing FTP story
- OT DoS is no joke

Pentesting

- We loud
- Basic attack vectors
- Look at all vulnerabilities
- Please, please tell me you can see me
- Minimal time

Red team

- Stealth
- Adversary/APT emulation
- Set goal of what to target
- EDR/MDR evasion
- More time

Red team:

Pentester:

Phun timez with clients

- Scope creep
- “We wanted a red team…”
- “There was an incident…”
- You don’t need to justify your org’s security failures to me -- it is what it is

Cover your ass

- Screenshots can save your job
- You need a way to prove that you did the work and followed the methodology
- Again, protect yourself

Q4

- Do you like a lot of time off during the holidays?
- People don't plan well sometimes…

P0s3rs

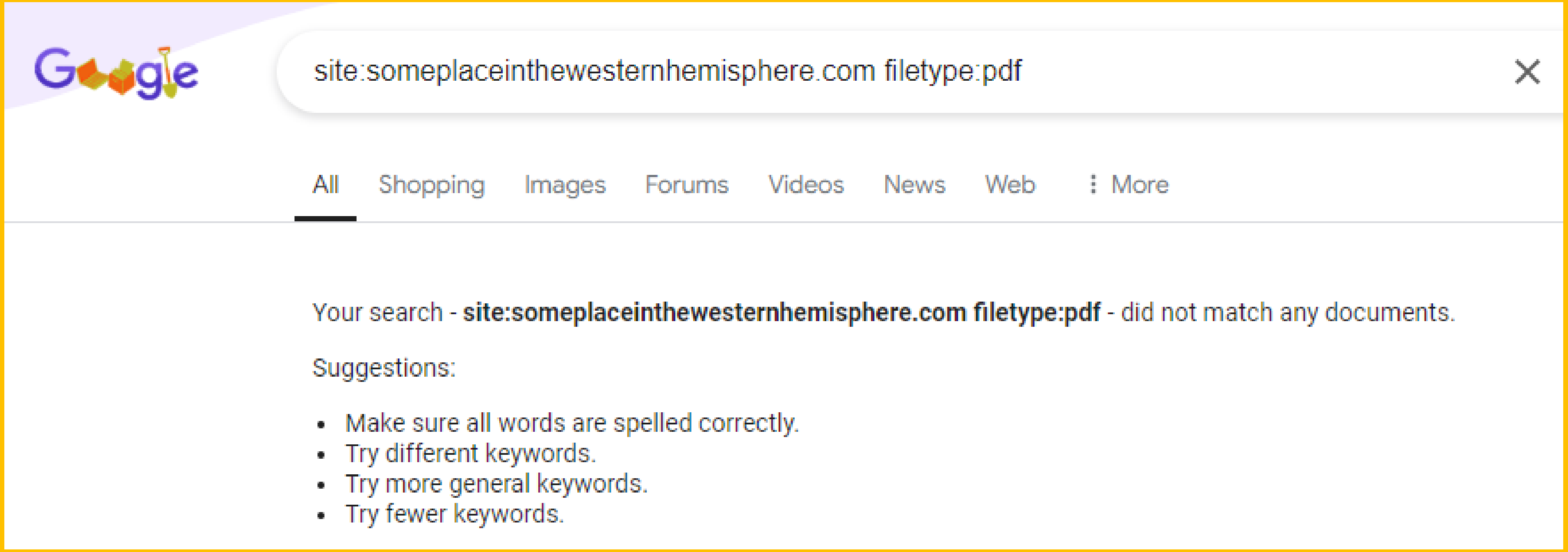
- A vulnerability scan is not a f%@#ing pentest
- Clean up after yourself!
- Neat trick to see if you might have been ripped off

Let’s talk about disclosures and CVEs….

- The CVE “ecosystem” is a disheveled mess
- Lack of verification, bogus or disputed CVEs
- Thousands of vulnerabilities do not have a CVE ID…
- What happens when you find a vuln?

What I’m seeing (externals)

- Information leakage
- Misconfigurations or default settings
- Outdated software

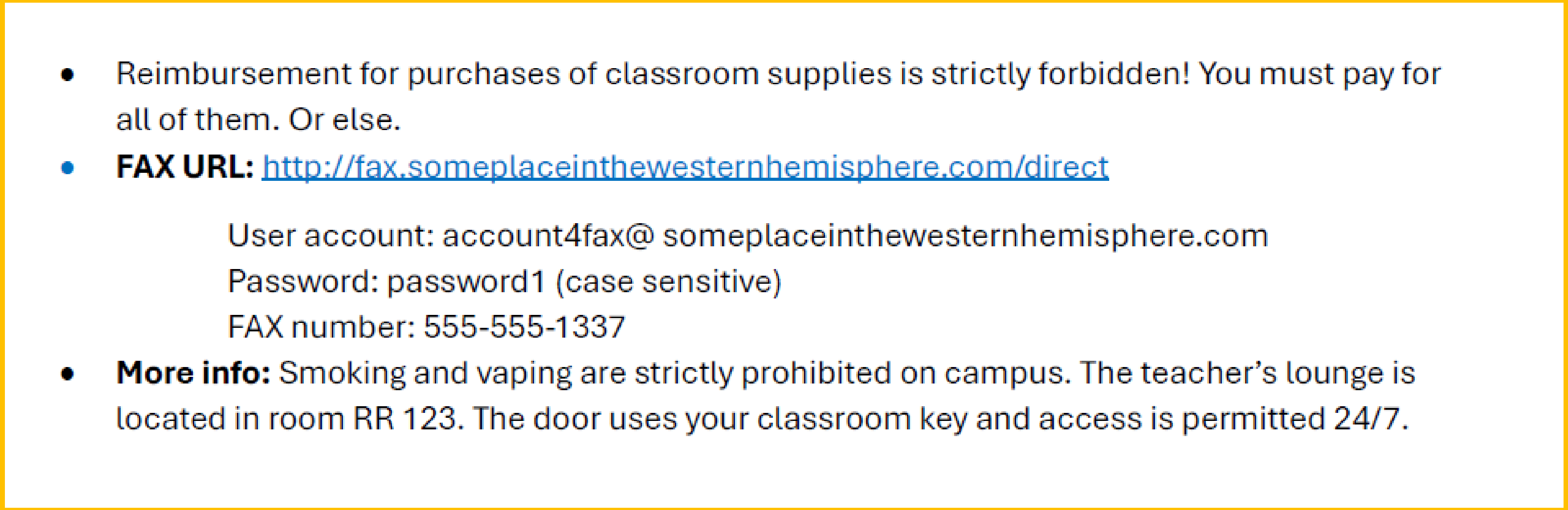


site:someplaceinthewesternhemisphere.com filetype:pdf

Your search - **site:someplaceinthewesternhemisphere.com filetype:pdf** - did not match any documents.

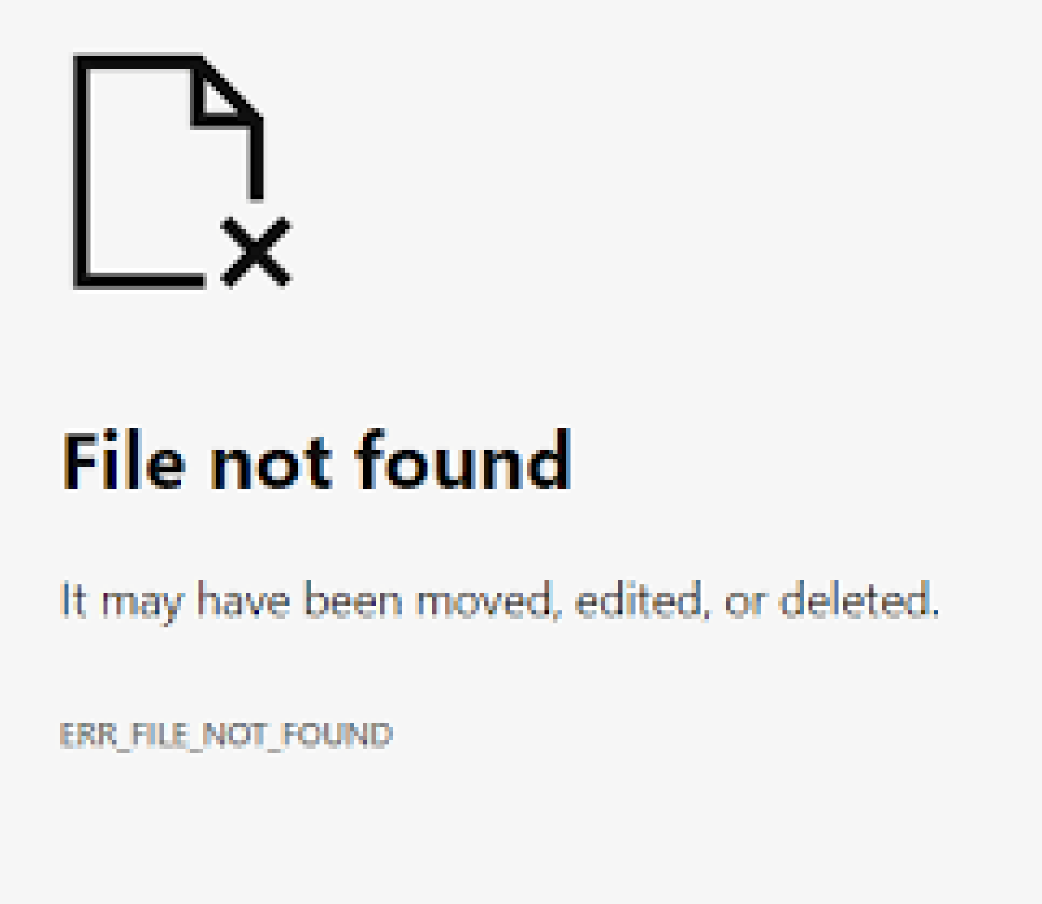
Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.



- Reimbursement for purchases of classroom supplies is strictly forbidden! You must pay for all of them. Or else.
- **FAX URL:** http://fax.someplaceinthewesternhemisphere.com/direct

  User account: account4fax@ someplaceinthewesternhemisphere.com
  Password: password1 (case sensitive)
  FAX number: 555-555-1337
- **More info:** Smoking and vaping are strictly prohibited on campus. The teacher’s lounge is located in room RR 123. The door uses your classroom key and access is permitted 24/7.



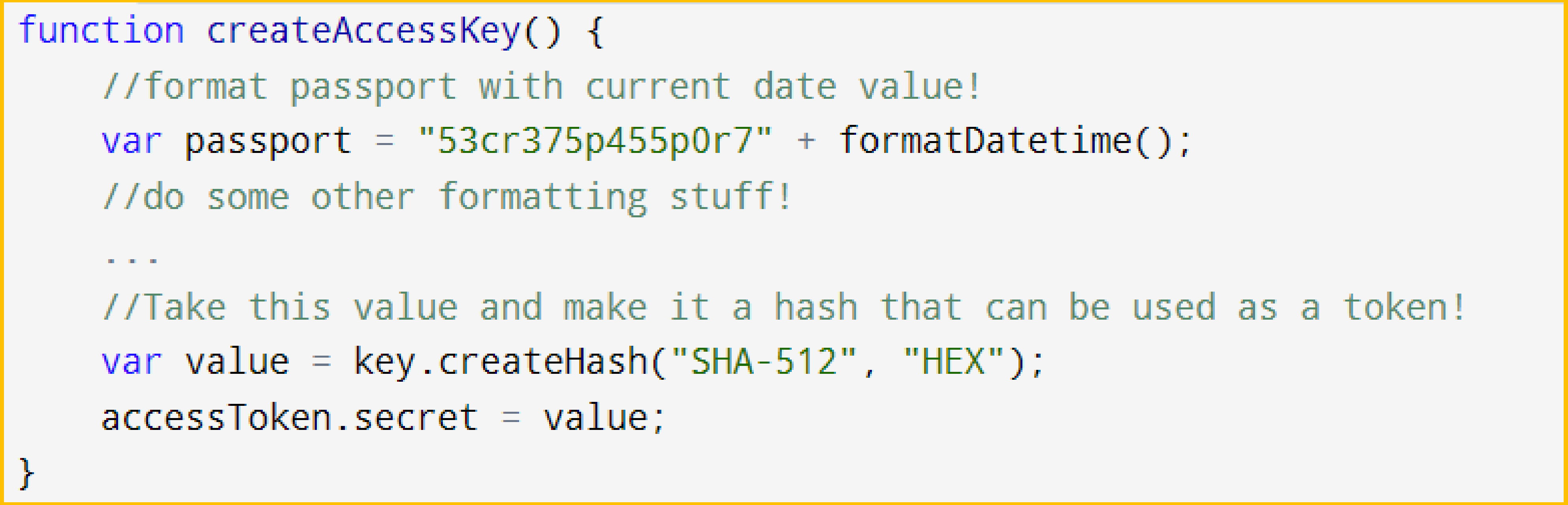
File not found

It may have been moved, edited, or deleted.

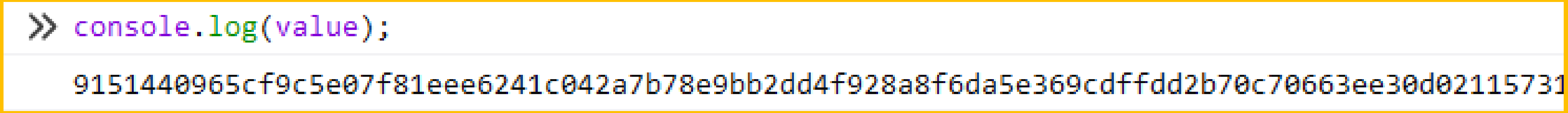
ERR_FILE_NOT_FOUND

What I’m seeing (apps)

- Broken access control, especially with APIs
- Authentication bypass



```javascript
function createAccessKey() {
    //format passport with current date value!
    var passport = "53cr375p455p0r7" + formatDatetime();
    //do some other formatting stuff!
    ...
    //Take this value and make it a hash that can be used as a token!
    var value = key.createHash("SHA-512", "HEX");
    accessToken.secret = value;
}
```



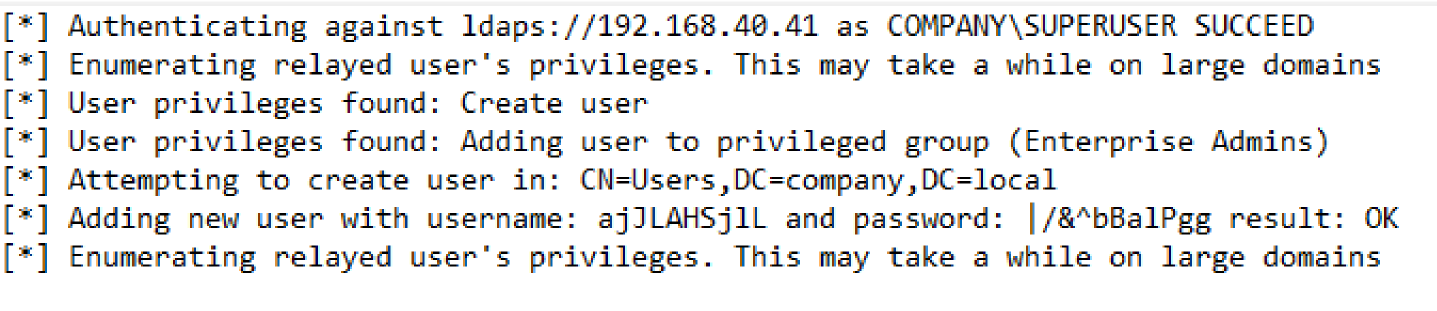
```
>> console.log(value);
   9151440965cf9c5e07f81eee6241c042a7b78e9bb2dd4f928a8f6da5e369cdffdd2b70c70663ee30d02115731
```

Hash value + POST request with SOAP API == UserToken value

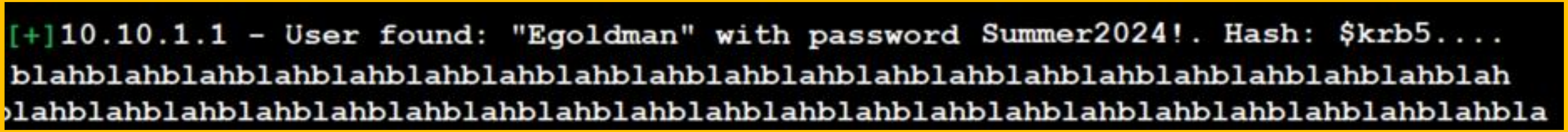
```
    <soap:Body>
        <m:FileIDDownload>
            <m:UserToken>
                dG+WxseXJhbmRvbW5vbnNlbnNlc3RyaW5nZGVmdG90YdGhpbmxpZW50Y
            </m:UserToken>
            <m:IdentityOfFile>
                45464614
            </m:IdentityOfFile>
        </m:FileIDDownload>
    </soap:Body>
```

What I’m seeing (internals)

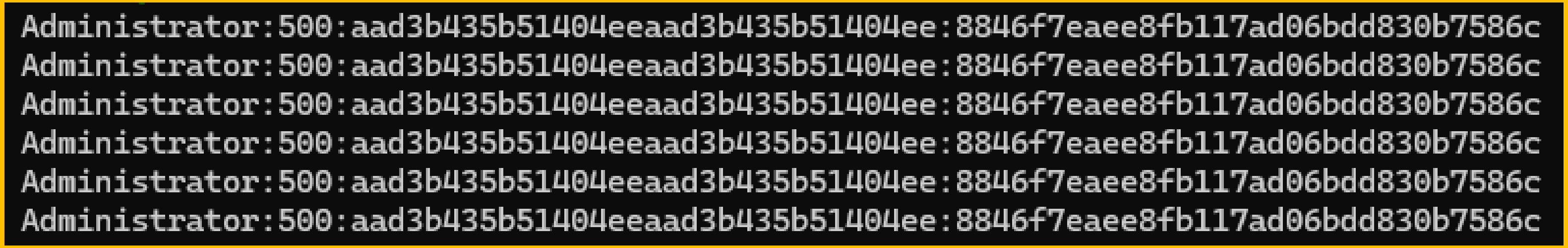
- SMB and/or LDAP/S relaying nearly every. single. time.
- Password reuse (*including* local Admin) or guessable passwords
- Service accounts that do not need DA privs… that result in me getting DA privs… (bonus if the password is set to not expire)



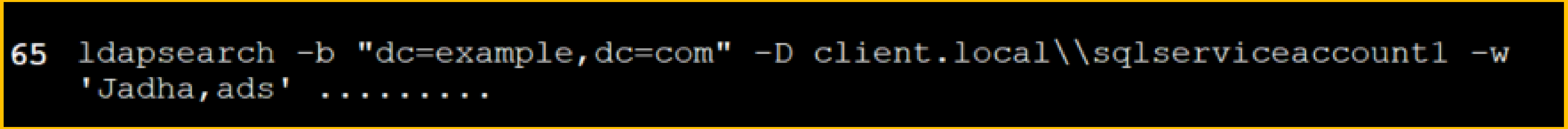
```
[*] Authenticating against ldaps://192.168.40.41 as COMPANY\SUPERUSER SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] User privileges found: Create user
[*] User privileges found: Adding user to privileged group (Enterprise Admins)
[*] Attempting to create user in: CN=Users,DC=company,DC=local
[*] Adding new user with username: ajJLAHSjlL and password: |/&^bBalPgg result: OK
[*] Enumerating relayed user's privileges. This may take a while on large domains
```



```
[+]10.10.1.1 - User found: "Egoldman" with password Summer2024!. Hash: $krb5....
blahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblah
lahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahbla
```



```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
```



```
65  ldapsearch -b "dc=example,dc=com" -D client.local\\sqlserviceaccount1 -w
    'Jadha,ads' .........
```

Making a difference?

- Protecting others?
- Providing helpful direction, not changing the world (usually)
- You are often a living, breathing checkbox

Heavy lifters

- Fixing, building, and rebuilding is the real, invaluable work
- Sys admins, security engineers, IR, analysts, etc.
- Pay them well

FIN

ACK

Thank You

Slides

- https://github.com/Hackerbartender/talkslides