Digital Certificates Fails and Flounders

Jeff Krakenberg jeffkraken @abandonfreewifi

1

What does this talk cover?

1) Digital Certificates (Overview) 🧑

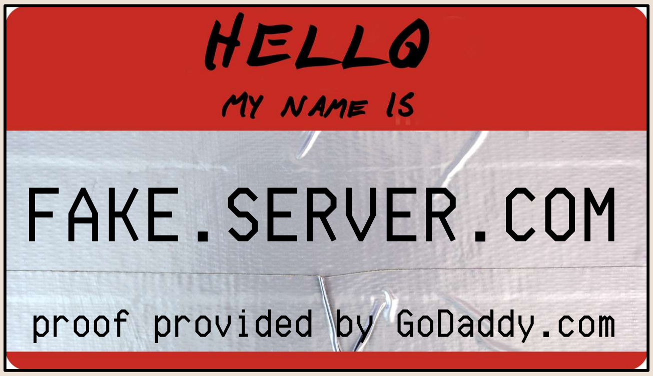
2) Fails 🏃 + 🦷

3) Flounders 🔥🧱

4) Digital Certificates (Wrap-up) 📜

2

What is a Digital Certificate?



A special type of file that identifies a resource, cryptographically.

1

3

Why does that matter?

2

4

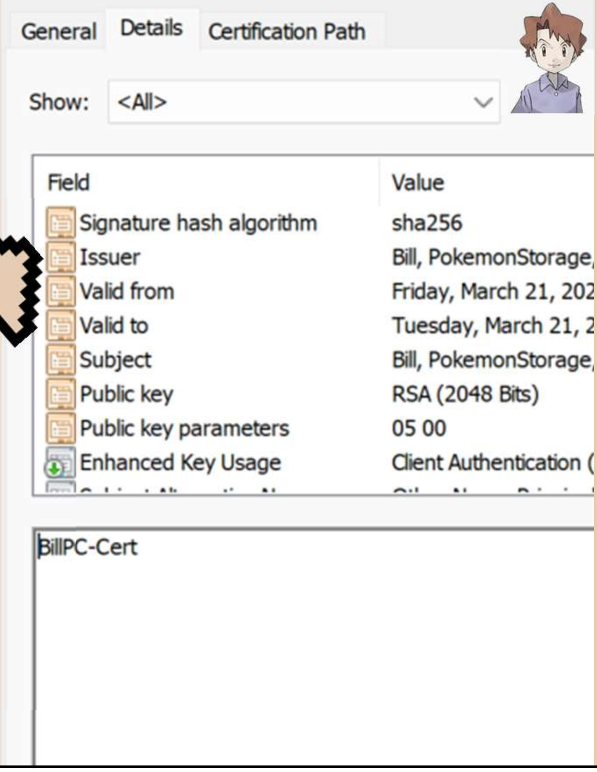
Why does that matter?

Digital Certificate: Mr. Pigeon
Jeff realizes their mistake and says: “Oh, sorry, Mr. Pigeon.”

3

5

How does this help?


General | Details | Certification Path

Show: <All>

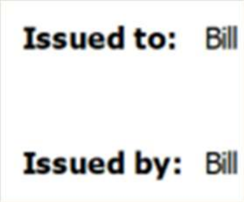
Field	Value
Signature hash algorithm	sha256
Issuer	Bill, PokemonStorage,
Valid from	Friday, March 21, 202
Valid to	Tuesday, March 21, 2
Subject	Bill, PokemonStorage,
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Client Authentication (

BillPC-Cert

4

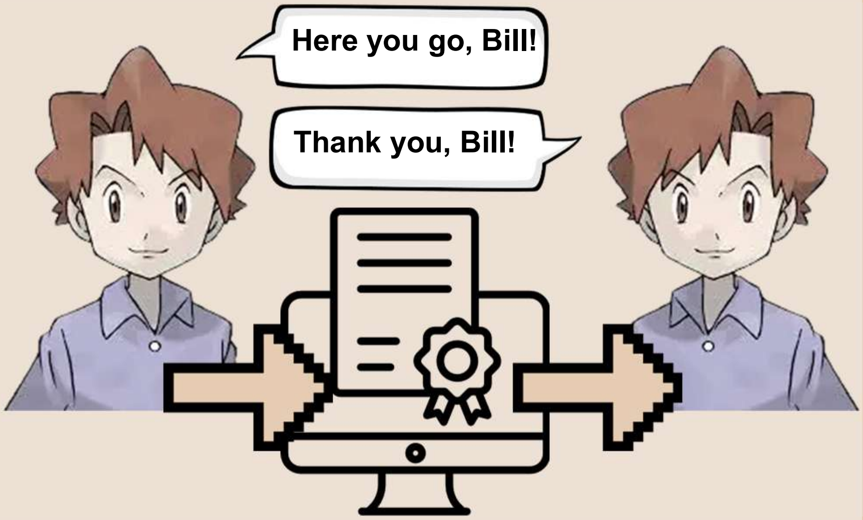
6

Should YOU trust Bill with your Pokémon?



Issued to: Bill

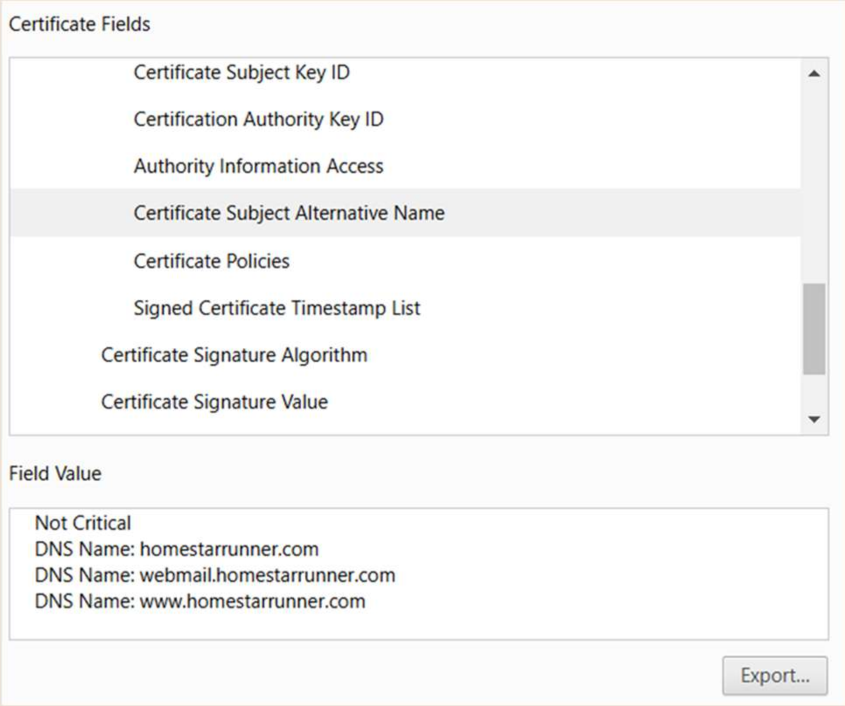
Issued by: Bill



5

7

Let’s fail: webmail



Certificate Fields

```
    Certificate Subject Key ID
    Certification Authority Key ID
    Authority Information Access
    Certificate Subject Alternative Name
    Certificate Policies
    Signed Certificate Timestamp List
  Certificate Signature Algorithm
  Certificate Signature Value
```

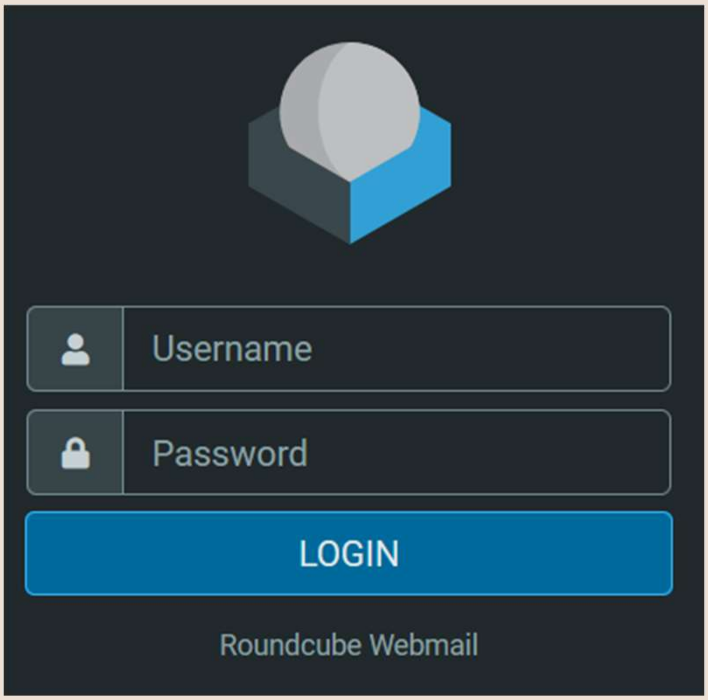
Field Value

```
Not Critical
DNS Name: homestarrunner.com
DNS Name: webmail.homestarrunner.com
DNS Name: www.homestarrunner.com
```

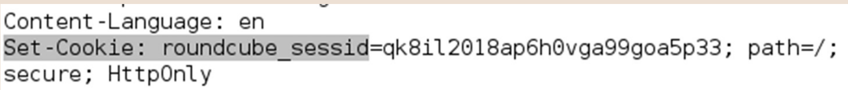
6

8

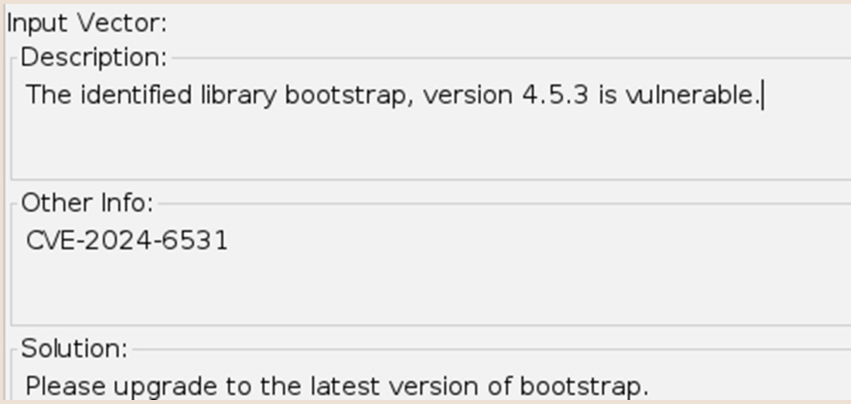
webmail:
admin access



webmail:
sessions
+ libraries



```
Content-Language: en
Set-Cookie: roundcube_sessid=qk8il2018ap6h0vga99goa5p33; path=/;
secure; HttpOnly
```



Input Vector:

Description:

The identified library bootstrap, version 4.5.3 is vulnerable.

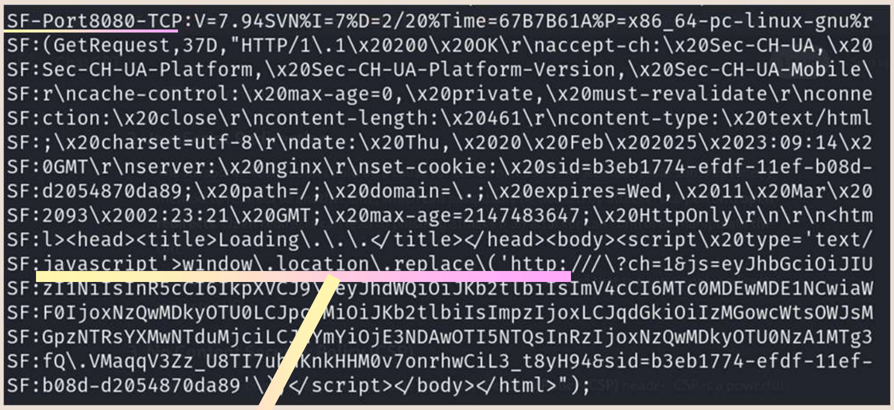
Other Info:

CVE-2024-6531

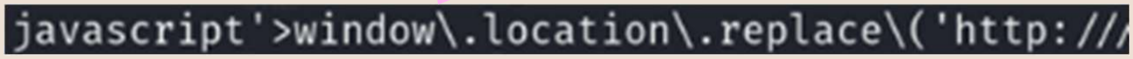
Solution:

Please upgrade to the latest version of bootstrap.

webmail: alt port + redirect

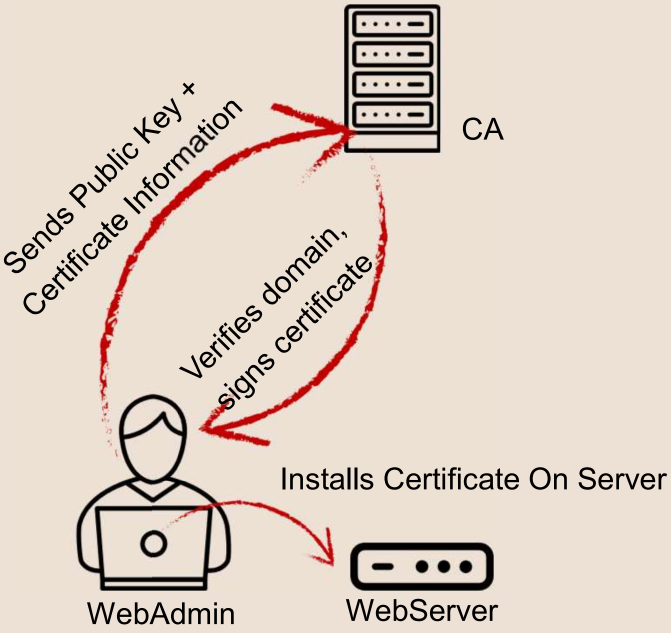


```
SF-Port8080-TCP:V=7.94SVN%I=7%D=2/20%Time=67B7B61A%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,37D,"HTTP/1\.1\x20200\x20OK\r\naccept-ch:\x20Sec-CH-UA,\x20
SF:Sec-CH-UA-Platform,\x20Sec-CH-UA-Platform-Version,\x20Sec-CH-UA-Mobile\
SF:r\ncache-control:\x20max-age=0,\x20private,\x20must-revalidate\r\nconne
SF:ction:\x20close\r\ncontent-length:\x20461\r\ncontent-type:\x20text/html
SF:;\x20charset=utf-8\r\ndate:\x20Thu,\x2020\x20Feb\x202025\x2023:09:14\x2
SF:0GMT\r\nserver:\x20nginx\r\nset-cookie:\x20sid=b3eb1774-efdf-11ef-b08d-
SF:d2054870da89;\x20path=/;\x20domain=\.;\x20expires=Wed,\x2011\x20Mar\x20
SF:2093\x2002:23:21\x20GMT;\x20max-age=2147483647;\x20HttpOnly\r\n\r\n<htm
SF:l><head><title>Loading\.\.\.</title></head><body><script\x20type='text/
SF:javascript'>window\.location\.replace\('http:///\?ch=1&js=eyJhbGciOiJIU
SF:zI1NiIsInR5cCI6IkpXVCJ9\.eyJhdWQiOiJKb2tlbiIsImV4cCI6MTc0MDEwMDE1NCwiaW
SF:F0IjoxNzQwMDkyOTU0LCJpc3MiOiJKb2tlbiIsImpzIjoxLCJqdGkiOiIzMGowcWtsOWJsM
SF:GpzNTRsYXMwNTduMjciLCJuYmYiOjE3NDAwOTI5NTQsInRzIjoxNzQwMDkyOTU0NzA1MTg3
SF:fQ\.VMaqqV3Zz_U8TI7ub KnkHHM0v7onrhwCiL3_t8yH94&sid=b3eb1774-efdf-11ef-
SF:b08d-d2054870da89'\);</script></body></html>");
```



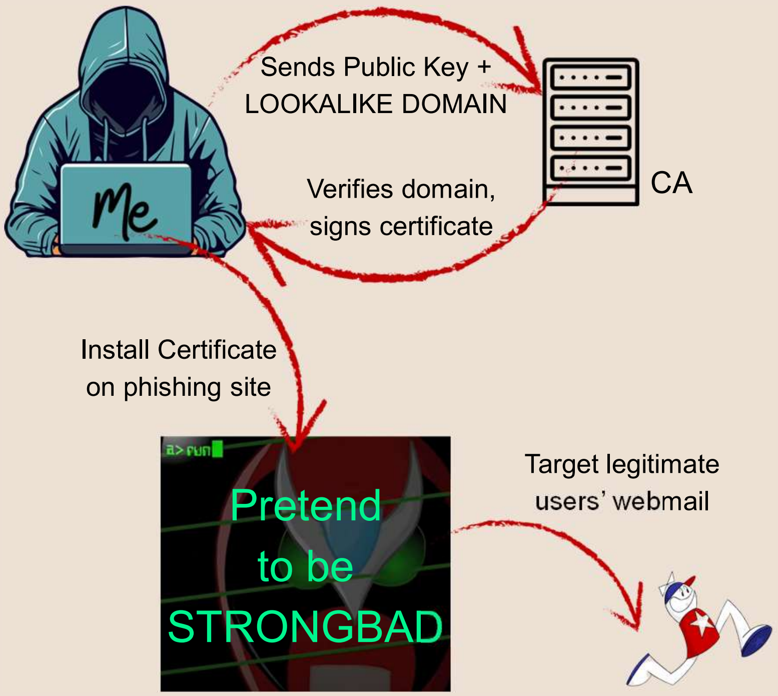
```
javascript'>window\.location\.replace\('http://
```

webmail: Core Issue

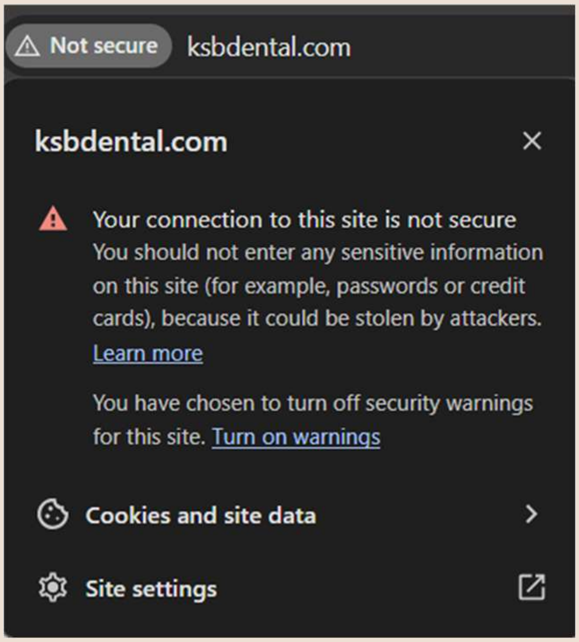


CA
Sends Public Key + Certificate Information
Verifies domain, signs certificate
Installs Certificate On Server
WebAdmin
WebServer

webmail: PHISHED x STRONGBAD



Let's fail again: Dental Redirect



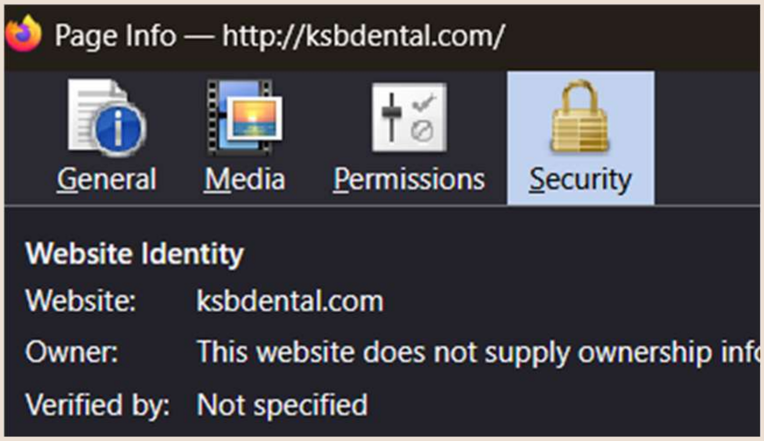
ksbdental.com ✕

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to turn off security warnings for this site. Turn on warnings

Dental Redirect: HTTP on Main?



Page Info — http://ksbdental.com/

Website Identity

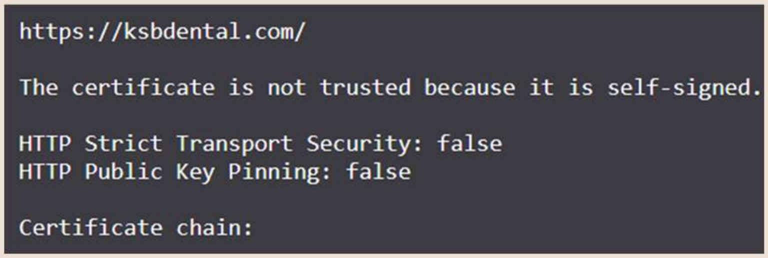
Website: ksbdental.com

Owner: This website does not supply ownership inf

Verified by: Not specified

15

Dental Redirect: If at first you don’t HTTPS, try HTTPS again.

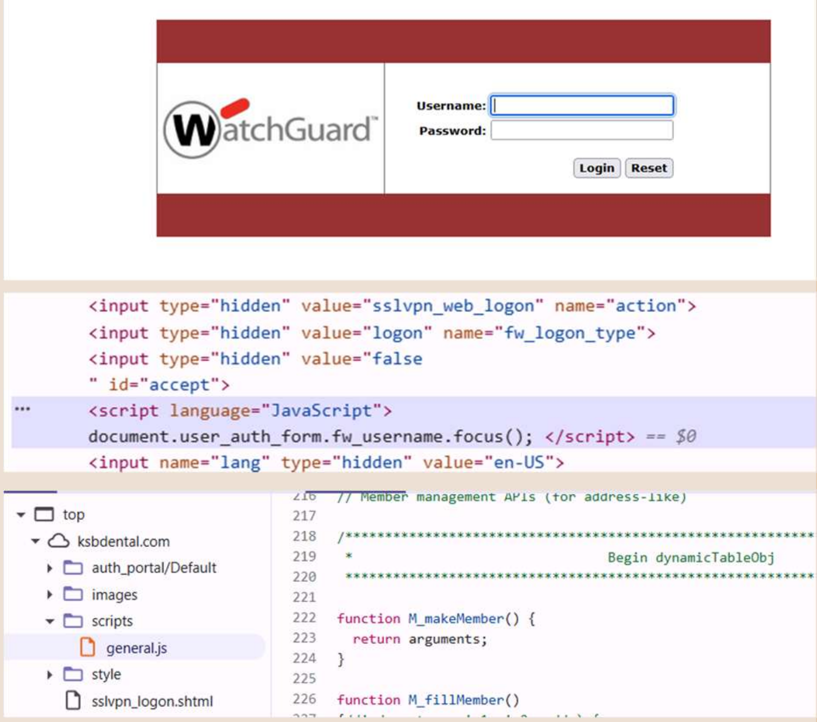


```
https://ksbdental.com/

The certificate is not trusted because it is self-signed.

HTTP Strict Transport Security: false
HTTP Public Key Pinning: false

Certificate chain:
```

14

16

Dental Redirect: What the watchguard?



```
<input type="hidden" value="sslvpn_web_logon" name="action">
<input type="hidden" value="logon" name="fw_logon_type">
<input type="hidden" value="false
" id="accept">
<script language="JavaScript">
document.user_auth_form.fw_username.focus(); </script> == $0
<input name="lang" type="hidden" value="en-US">
```

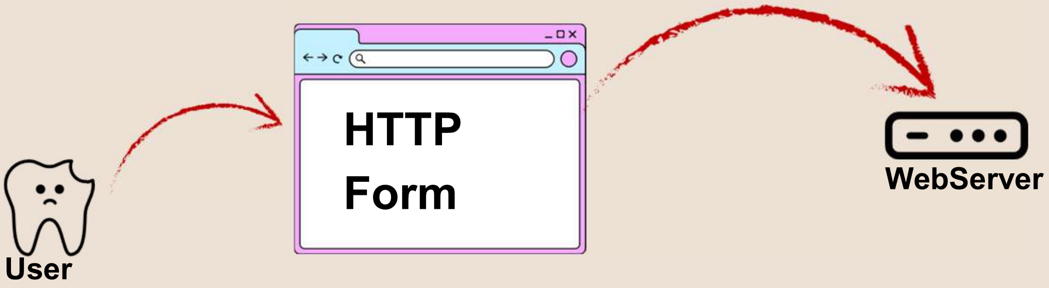
```
top
  ksbdental.com
    auth_portal/Default
    images
    scripts
      general.js
    style
    sslvpn_logon.shtml
```

```
// Member management APIs (for address-like)

/***********************************************************
 *                                  Begin dynamicTableObj
 ***********************************************************

function M_makeMember() {
  return arguments;
}

function M_fillMember()
```

15

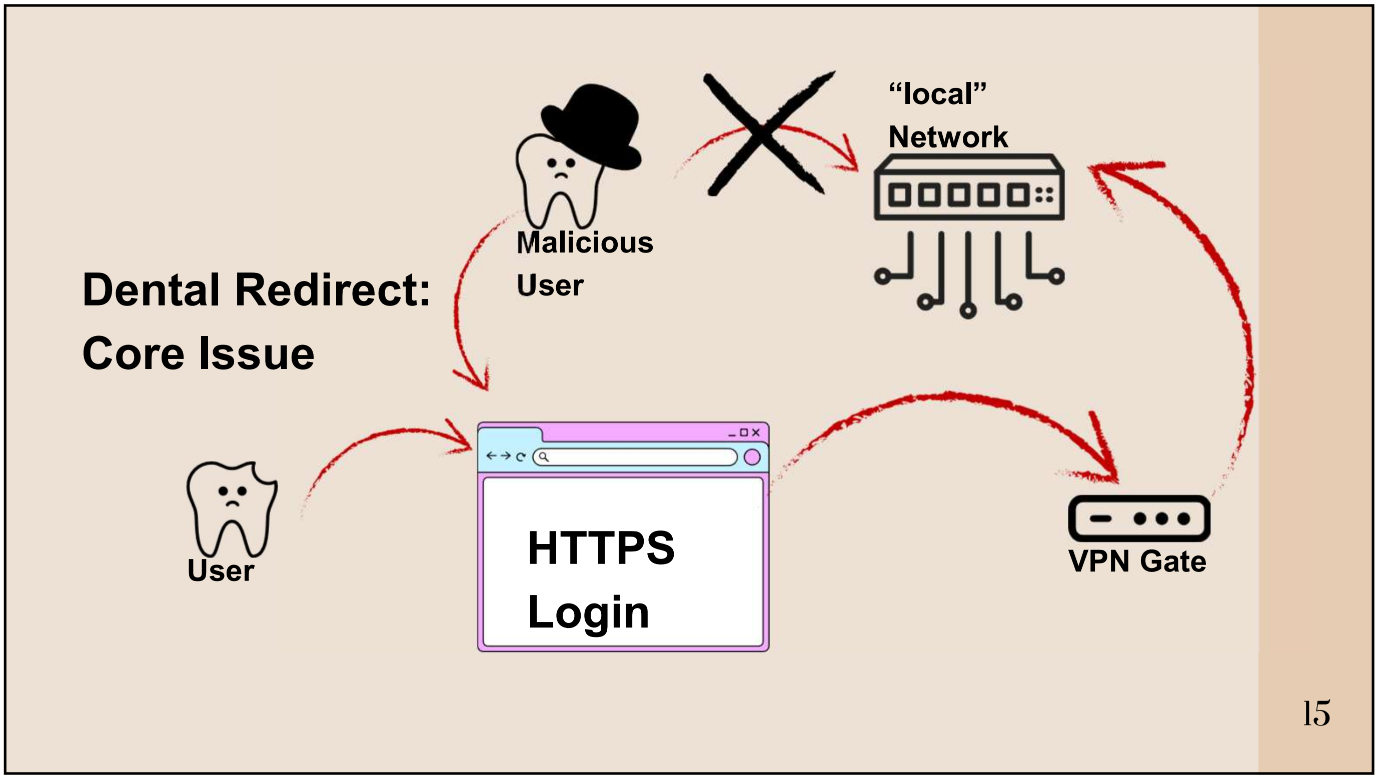
17

Dental Redirect: Core Issue



15

18



Dental Redirect: Core Issue

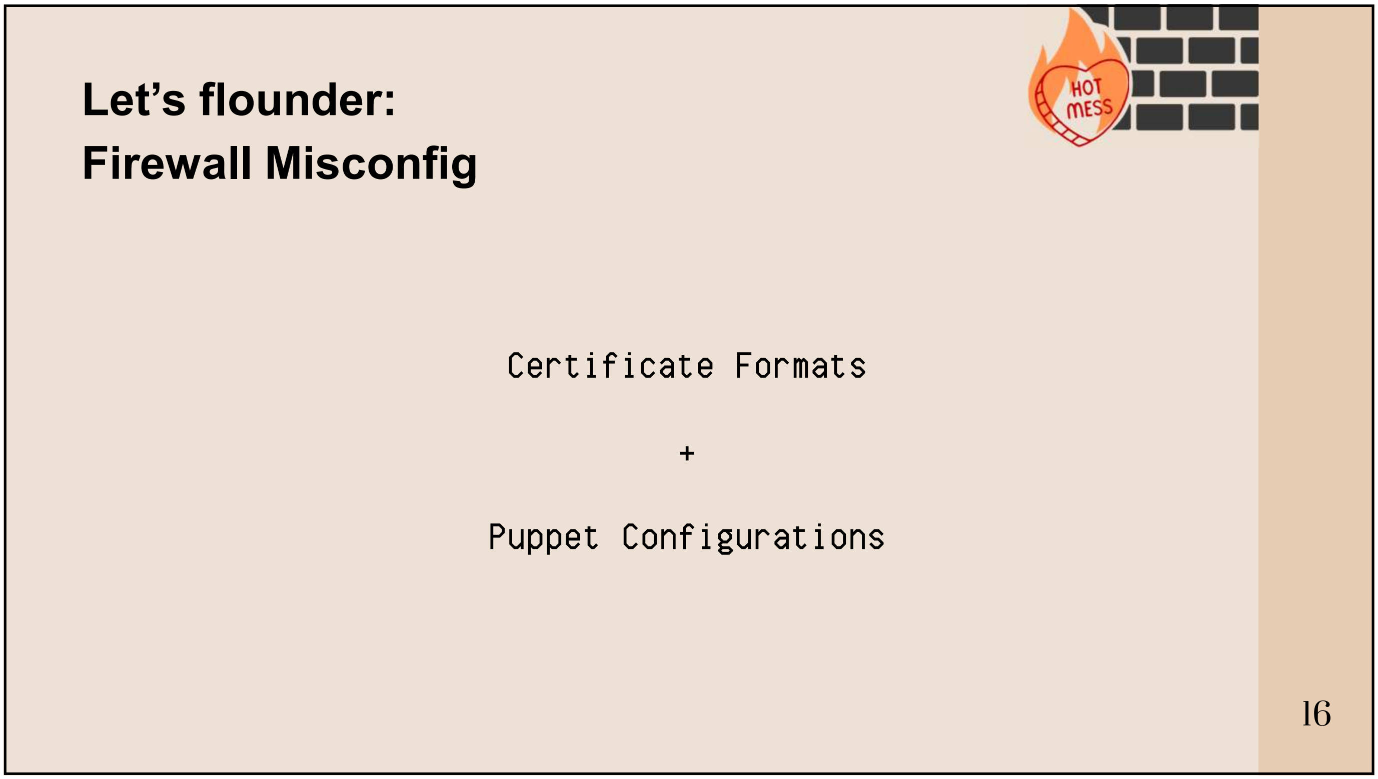
Malicious User

“local” Network

User

HTTPS Login

VPN Gate



Let’s flounder: Firewall Misconfig

Certificate Formats

+

Puppet Configurations

Firewall Misconfig:
Cert Format

- Linux Certs
  - File Format: .crt
- Fix: openssl:

```
openssl x509 \
–inform PEM \
–in “cert.cer” \
–out cert.crt
```

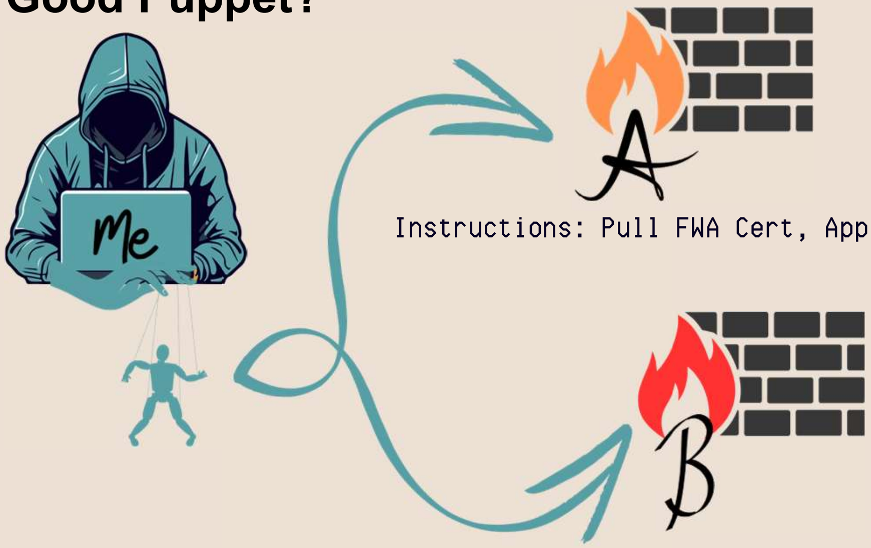
- Windows Certs
  - File Format: .cer
- Fix: Powershell:

```
$cert = get-childitem “cert.crt”
export-certificate `
–cert $cert `
–filepath “cert.cer”
```

17

21

Firewall Misconfig:
Good Puppet?



Instructions: Pull FWA Cert, Apply FWA Cert to FWA

Instructions: Pull FWB Cert, Apply FWB Cert to FWB

18

22

Firewall Misconfig: Bad Puppet!

```
file { "/etc/ssl/certs/$Firewall_A-cert.crt":
source => "puppet:///modules/firewall/certs/${firewall::certificates[$Firewall_A]}",
mode => '0644’, }
if $::hostname == $Firewall_B {
file { "/etc/ssl/certs/${::hostname}-cert.crt":
source => "puppet:///modules/firewall/certs/${firewall::certificates[$::hostname]}",
mode => '0644', } }
```

19

23

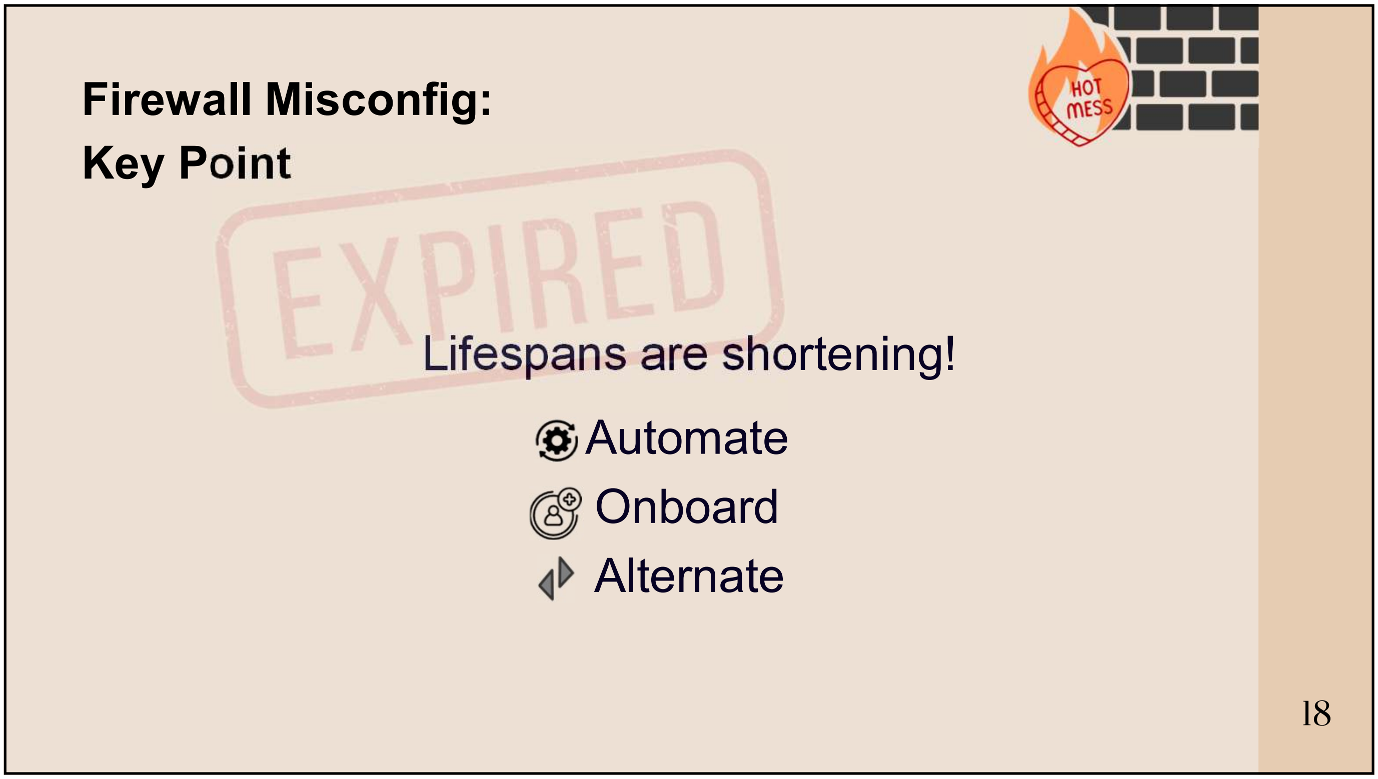
Firewall Misconfig: Key Point

EXPIRED

- Current: 398 Days
- March ‘26: 200 Days
- March ‘29: 47 Days

24

24



Firewall Misconfig: Key Point

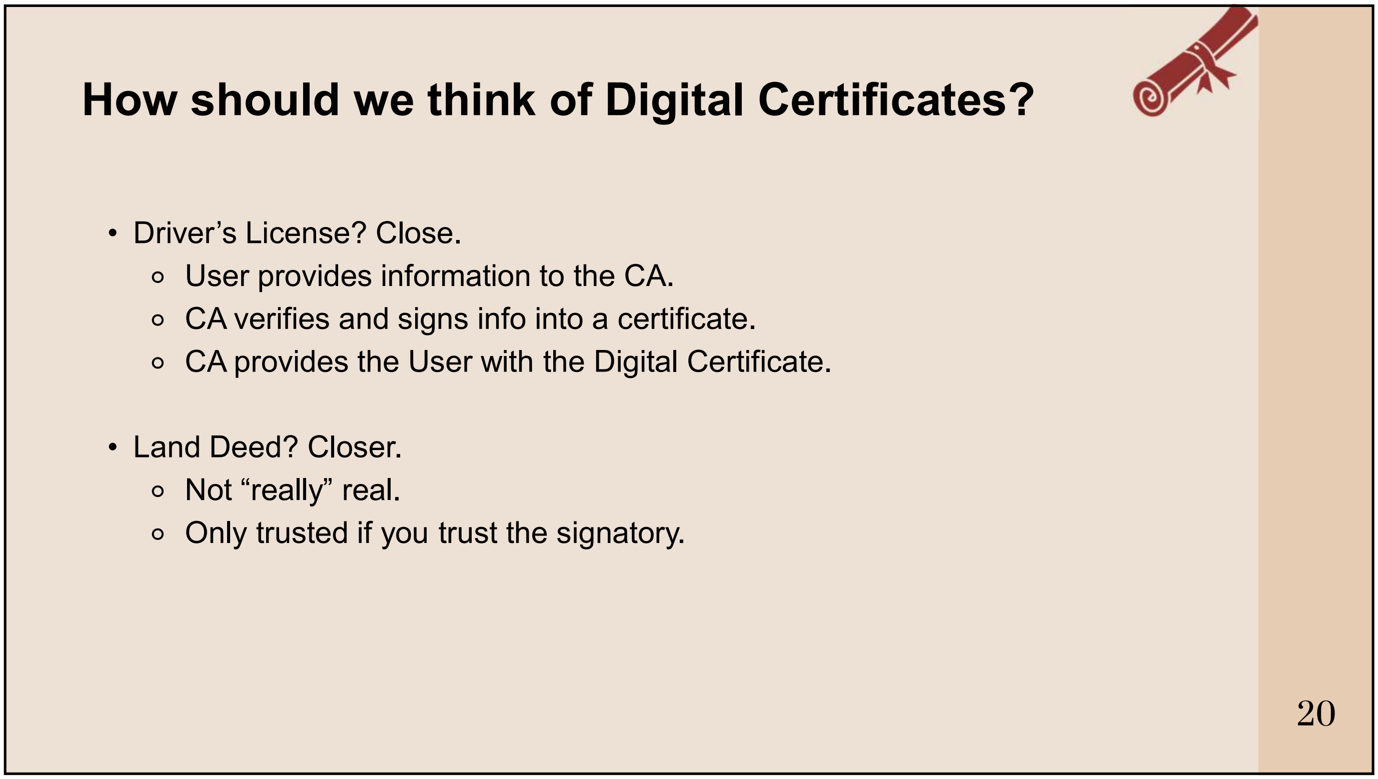
EXPIRED

Lifespans are shortening!

- Automate
- Onboard
- Alternate

18

25

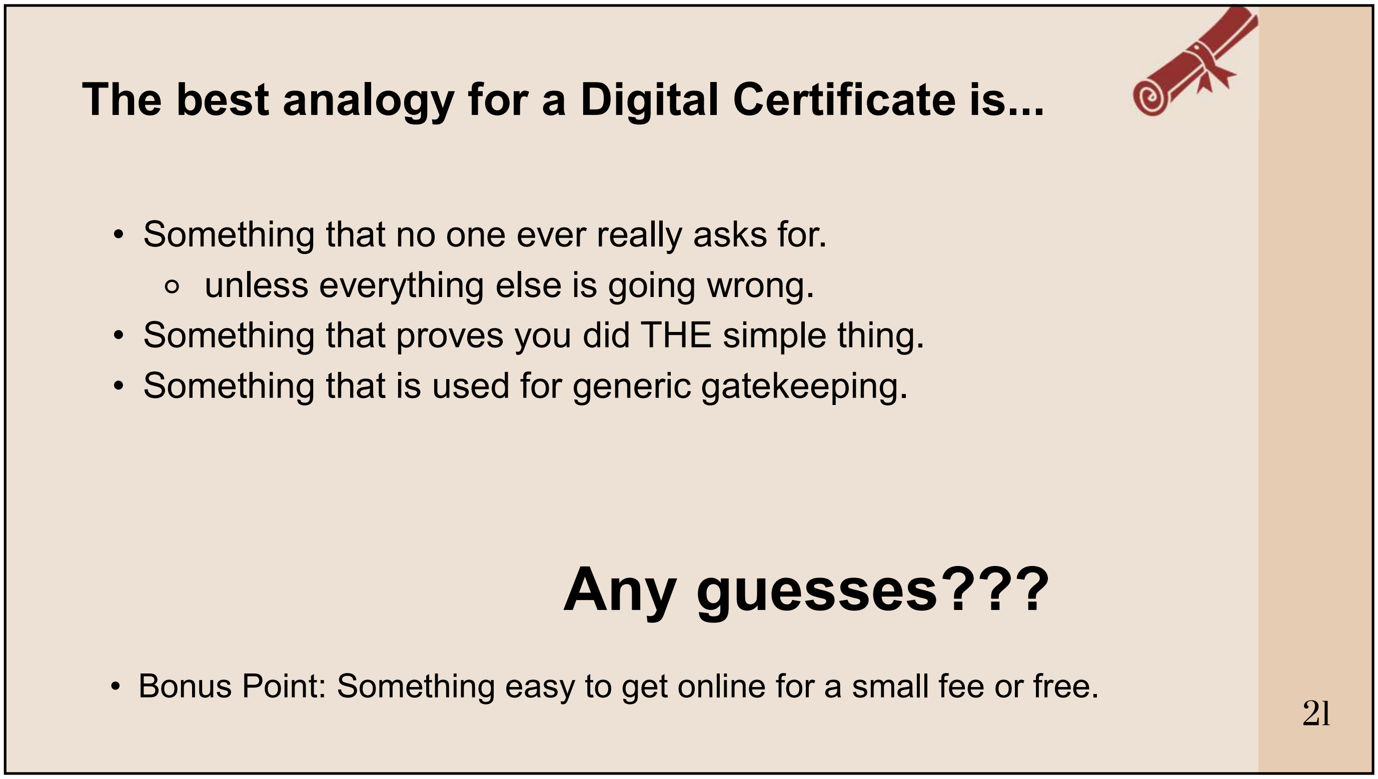


How should we think of Digital Certificates?

- Driver’s License? Close.
  - User provides information to the CA.
  - CA verifies and signs info into a certificate.
  - CA provides the User with the Digital Certificate.
- Land Deed? Closer.
  - Not “really” real.
  - Only trusted if you trust the signatory.

20

26



The best analogy for a Digital Certificate is...

- Something that no one ever really asks for.
  - unless everything else is going wrong.
- Something that proves you did THE simple thing.
- Something that is used for generic gatekeeping.

Any guesses???

- Bonus Point: Something easy to get online for a small fee or free.

21

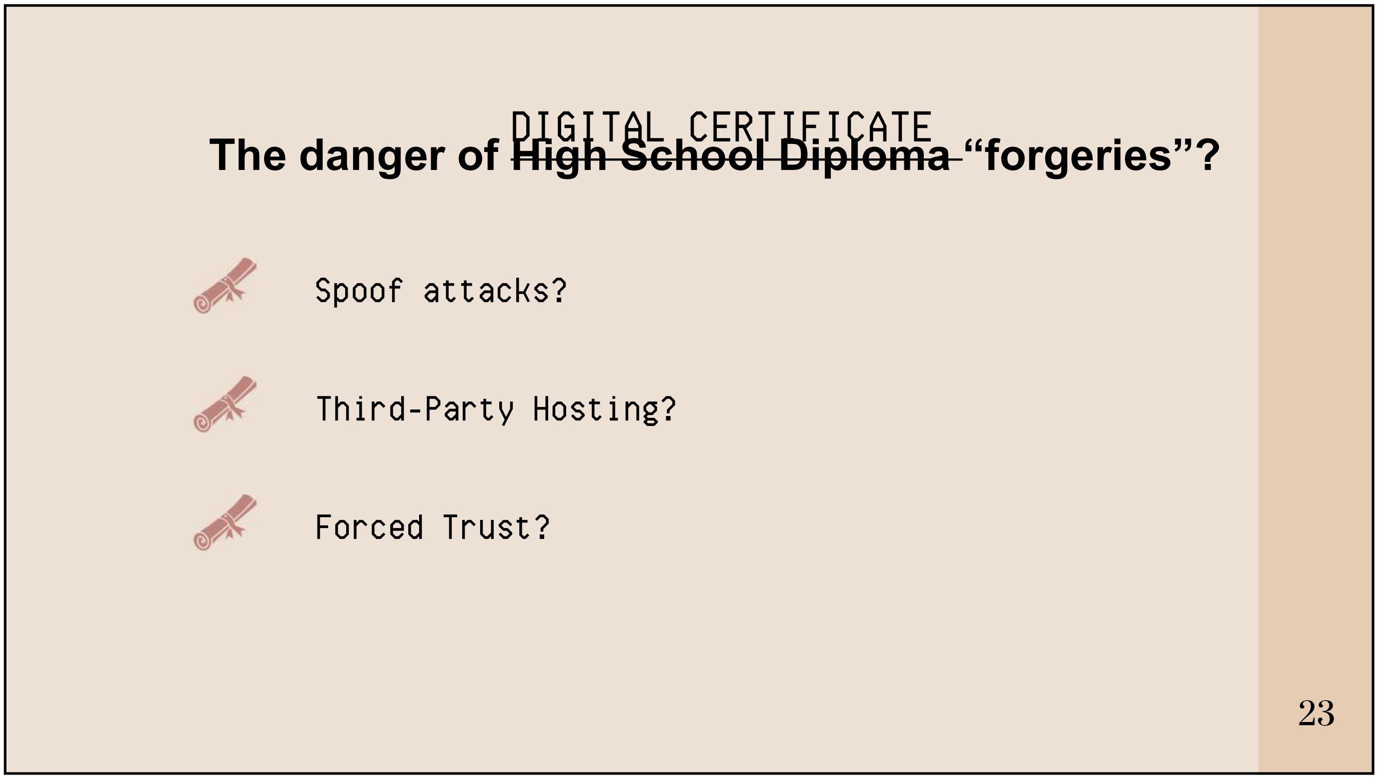
27

A better analogy for a Digital Certificate is...

High School Diploma

22

28

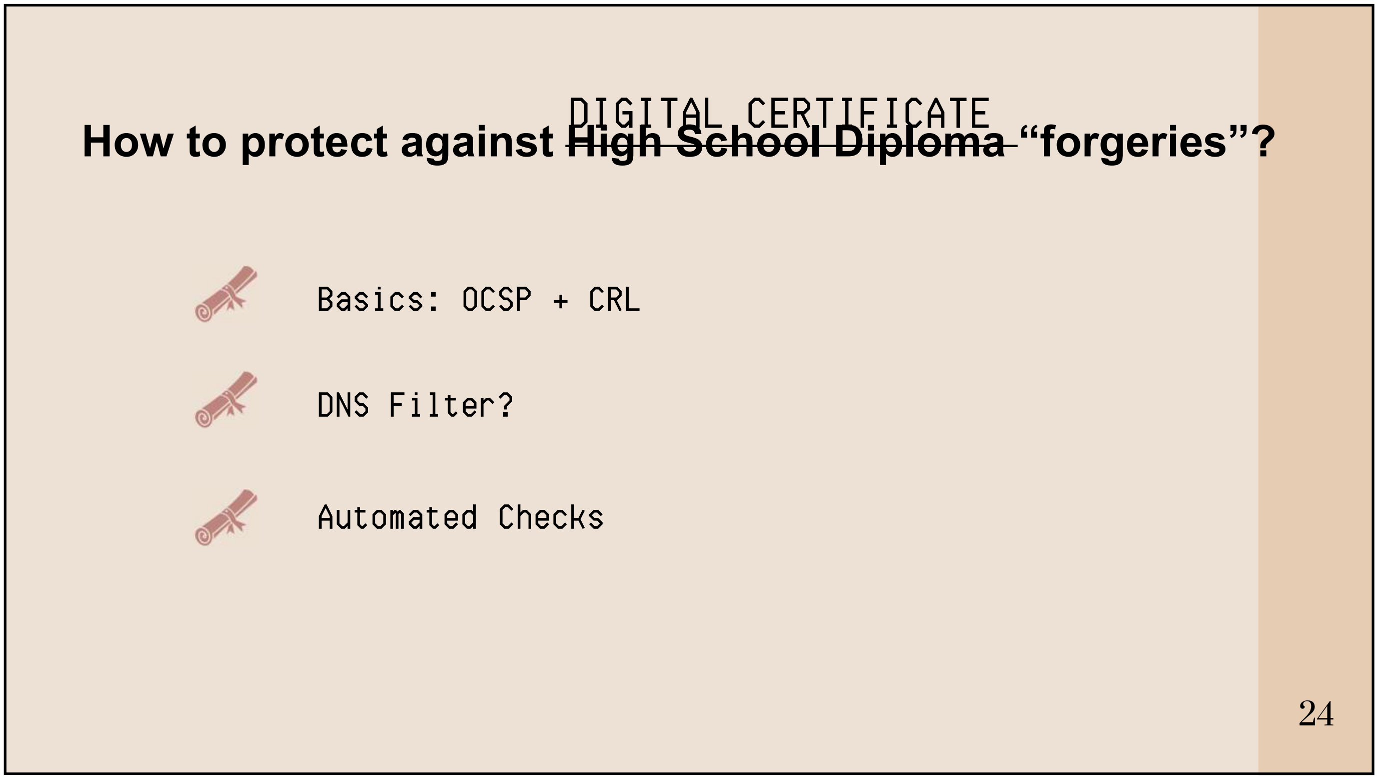


The danger of ~~High School Diploma~~ DIGITAL CERTIFICATE “forgeries”?

- Spoof attacks?
- Third-Party Hosting?
- Forced Trust?

23

29



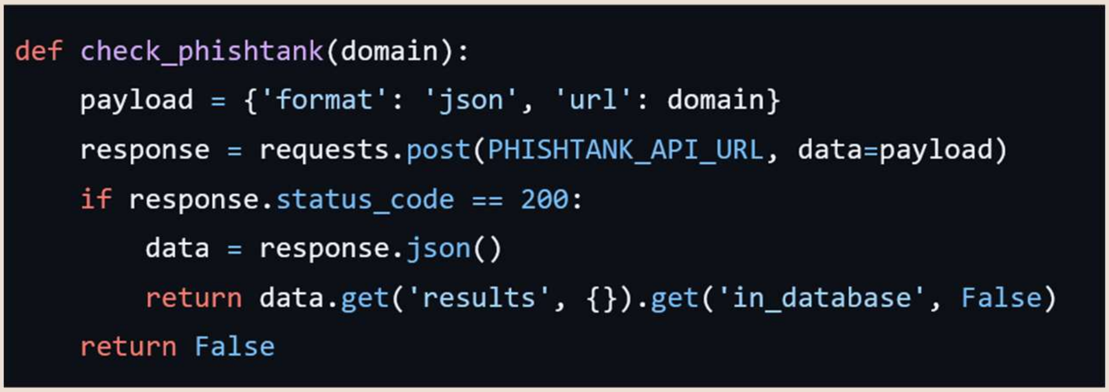
How to protect against ~~High School Diploma~~ DIGITAL CERTIFICATE “forgeries”?

- Basics: OCSP + CRL
- DNS Filter?
- Automated Checks

24

30

PhishTank

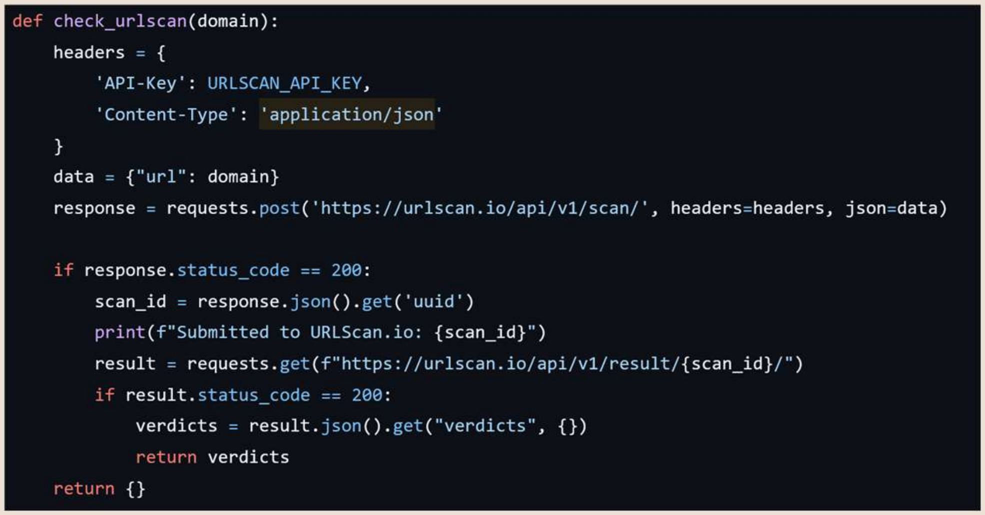


```python
def check_phishtank(domain):
    payload = {'format': 'json', 'url': domain}
    response = requests.post(PHISHTANK_API_URL, data=payload)
    if response.status_code == 200:
        data = response.json()
        return data.get('results', {}).get('in_database', False)
    return False
```

25

31

URLScan.io

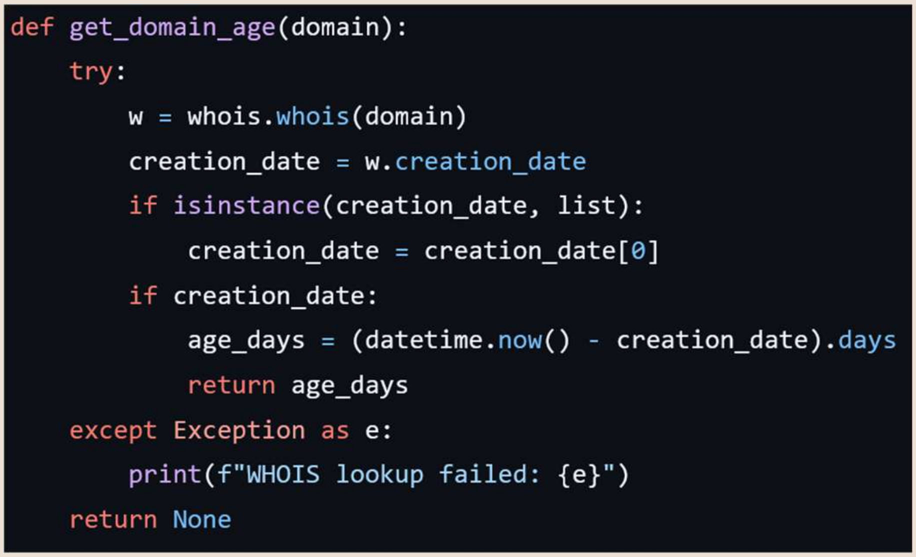


```python
def check_urlscan(domain):
    headers = {
        'API-Key': URLSCAN_API_KEY,
        'Content-Type': 'application/json'
    }
    data = {"url": domain}
    response = requests.post('https://urlscan.io/api/v1/scan/', headers=headers, json=data)

    if response.status_code == 200:
        scan_id = response.json().get('uuid')
        print(f"Submitted to URLScan.io: {scan_id}")
        result = requests.get(f"https://urlscan.io/api/v1/result/{scan_id}/")
        if result.status_code == 200:
            verdicts = result.json().get("verdicts", {})
            return verdicts
    return {}
```

26

32

Domain Age

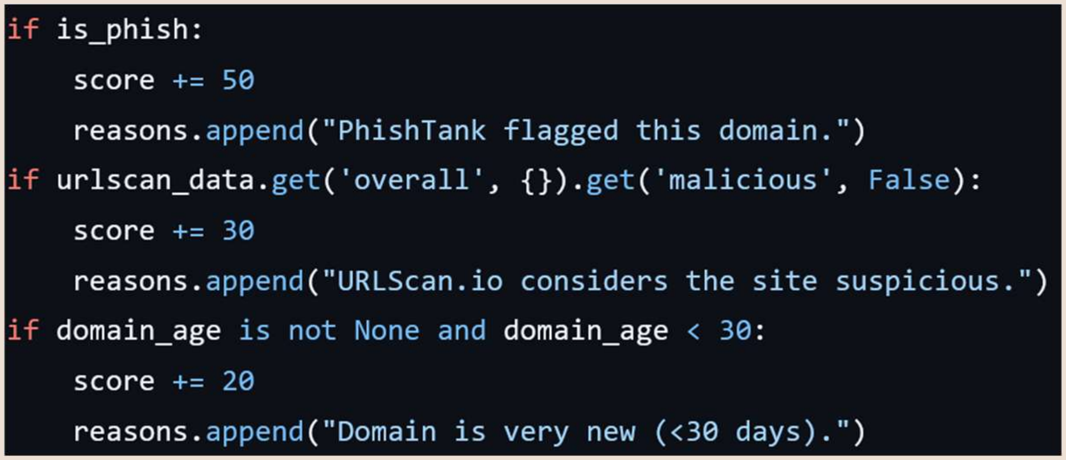


```
def get_domain_age(domain):
    try:
        w = whois.whois(domain)
        creation_date = w.creation_date
        if isinstance(creation_date, list):
            creation_date = creation_date[0]
        if creation_date:
            age_days = (datetime.now() - creation_date).days
            return age_days
    except Exception as e:
        print(f"WHOIS lookup failed: {e}")
    return None
```

24

33

“Scoring”



```
if is_phish:
    score += 50
    reasons.append("PhishTank flagged this domain.")
if urlscan_data.get('overall', {}).get('malicious', False):
    score += 30
    reasons.append("URLScan.io considers the site suspicious.")
if domain_age is not None and domain_age < 30:
    score += 20
    reasons.append("Domain is very new (<30 days).")
```

24

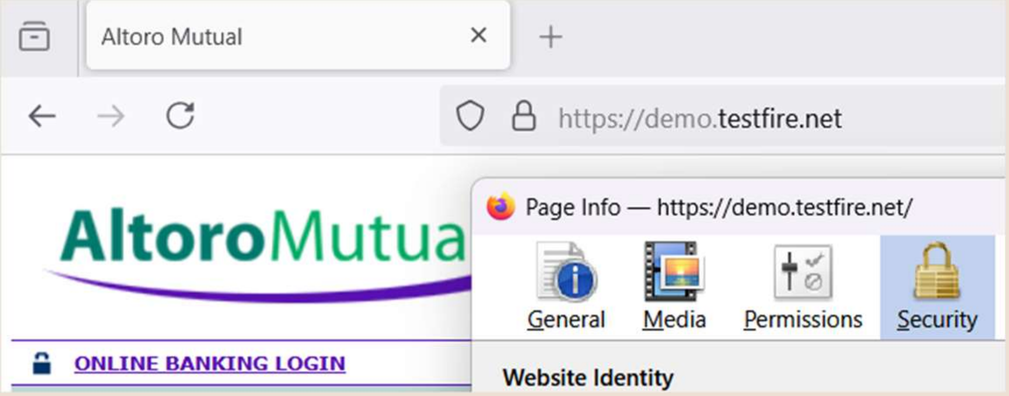
34

CERTIFICATE TRANSPARENCY LOGS

- What is a CT Log?
- How can these help?
- Example: CRT.SH

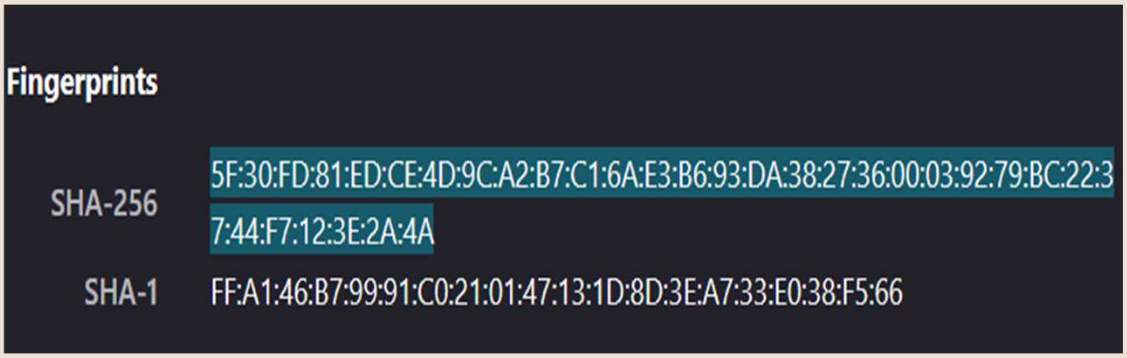
35

DEMO: CRT.SH - TESTFIRE



36

DEMO: CRT.SH - Certificate Fingerprint



Fingerprints

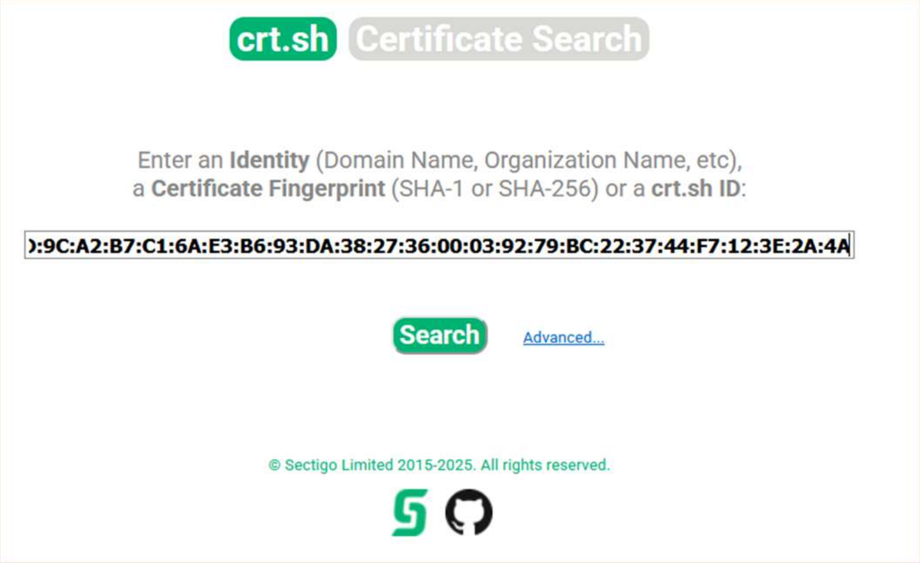
SHA-256 5F:30:FD:81:ED:CE:4D:9C:A2:B7:C1:6A:E3:B6:93:DA:38:27:36:00:03:92:79:BC:22:37:44:F7:12:3E:2A:4A

SHA-1 FF:A1:46:B7:99:91:C0:21:01:47:13:1D:8D:3E:A7:33:E0:38:F5:66

24

37

DEMO: CRT.SH - Certificate Search



Enter an **Identity** (Domain Name, Organization Name, etc),
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

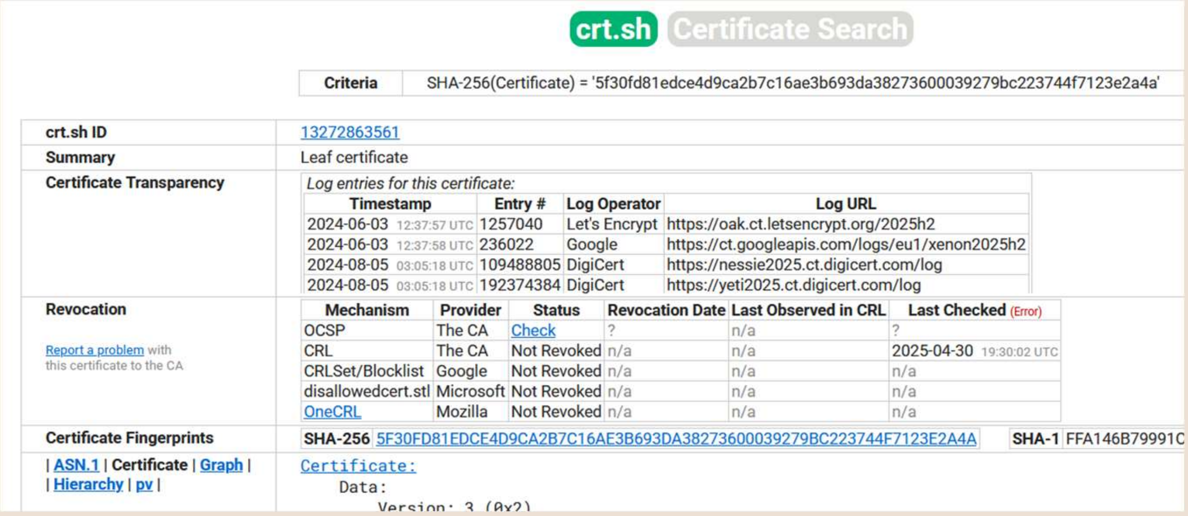
):9C:A2:B7:C1:6A:E3:B6:93:DA:38:27:36:00:03:92:79:BC:22:37:44:F7:12:3E:2A:4A

© Sectigo Limited 2015-2025. All rights reserved.

24

38

DEMO: CRT.SH - Certificate Search



crt.sh Certificate Search

Criteria	SHA-256(Certificate) = '5f30fd81edce4d9ca2b7c16ae3b693da38273600039279bc223744f7123e2a4a'

crt.sh ID	13272863561
Summary	Leaf certificate
Certificate Transparency	*Log entries for this certificate:*

Timestamp	Entry #	Log Operator	Log URL
2024-06-03 12:37:57 UTC	1257040	Let's Encrypt	https://oak.ct.letsencrypt.org/2025h2
2024-06-03 12:37:58 UTC	236022	Google	https://ct.googleapis.com/logs/eu1/xenon2025h2
2024-08-05 03:05:18 UTC	109488805	DigiCert	https://nessie2025.ct.digicert.com/log
2024-08-05 03:05:18 UTC	192374384	DigiCert	https://yeti2025.ct.digicert.com/log

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2025-04-30 19:30:02 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints **SHA-256** 5F30FD81EDCE4D9CA2B7C16AE3B693DA38273600039279BC223744F7123E2A4A **SHA-1** FFA146B79991C

| **ASN.1** | **Certificate** | **Graph** |
| **Hierarchy** | **pv** |

```
Certificate:
    Data:
        Version: 3 (0x2)
```

24

Thank you for your time!

Scan to connect, get a Digital “Digital Certificate” Certificate, or provide feedback.