Bank Grade Security

Bank Grade Security

Hello!

I am Kieran Jacobsen

My pronouns are he/him

You can find me at @kjacobsen

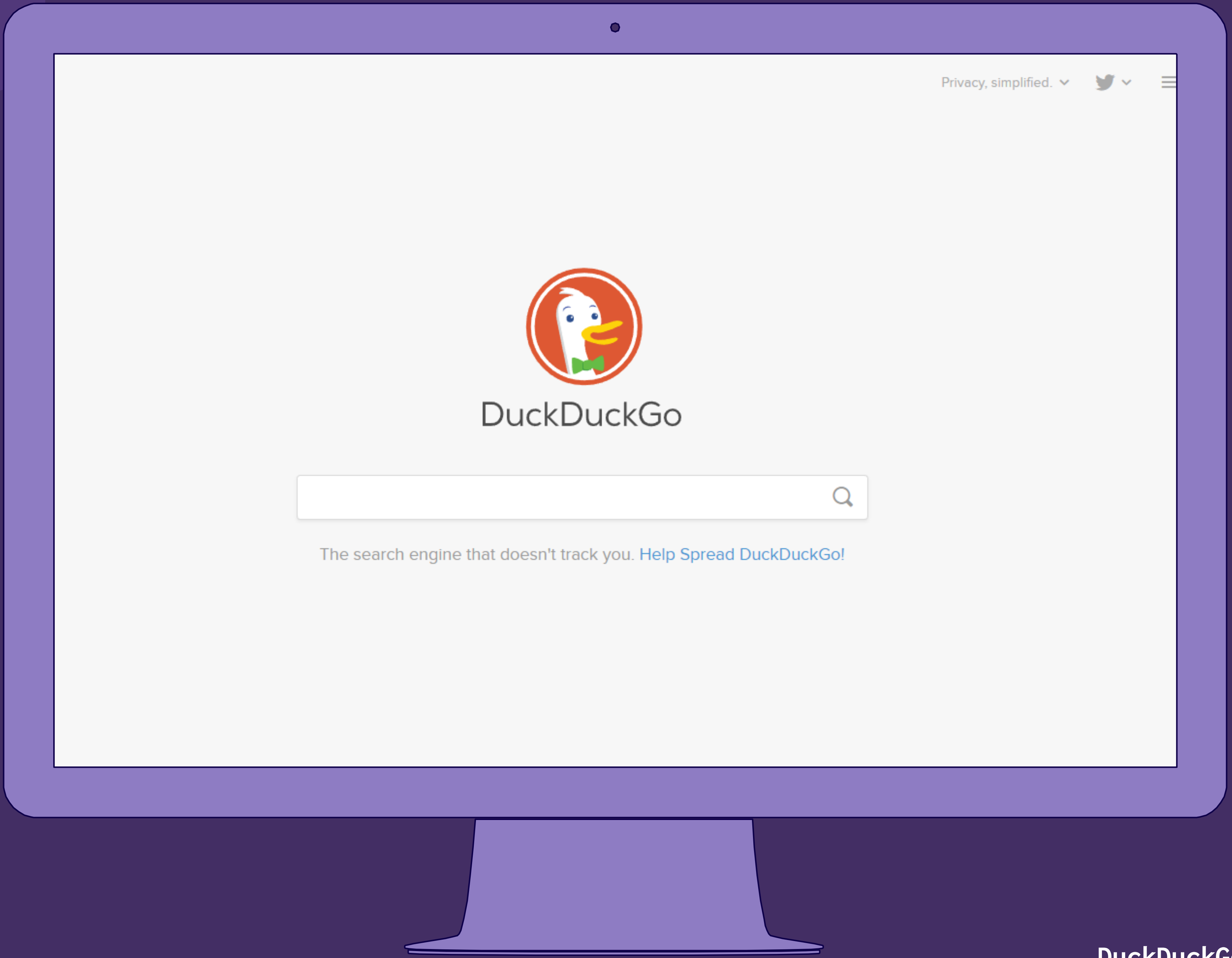
Photo source: WOCINTECHCHAT (wocintechchat.com)

Westpac
Commonwealth Bank
National Australia Bank
ANZ
Heritage Bank
bankwest
st.george
Bank of Melbourne
AMP
ING
SUNCORP
Bendigo Bank
BOQ
U BANK
bankSA

Photo sources: Wikipedia + Bank Websites

Photo sources: Wikipedia + Bank Websites

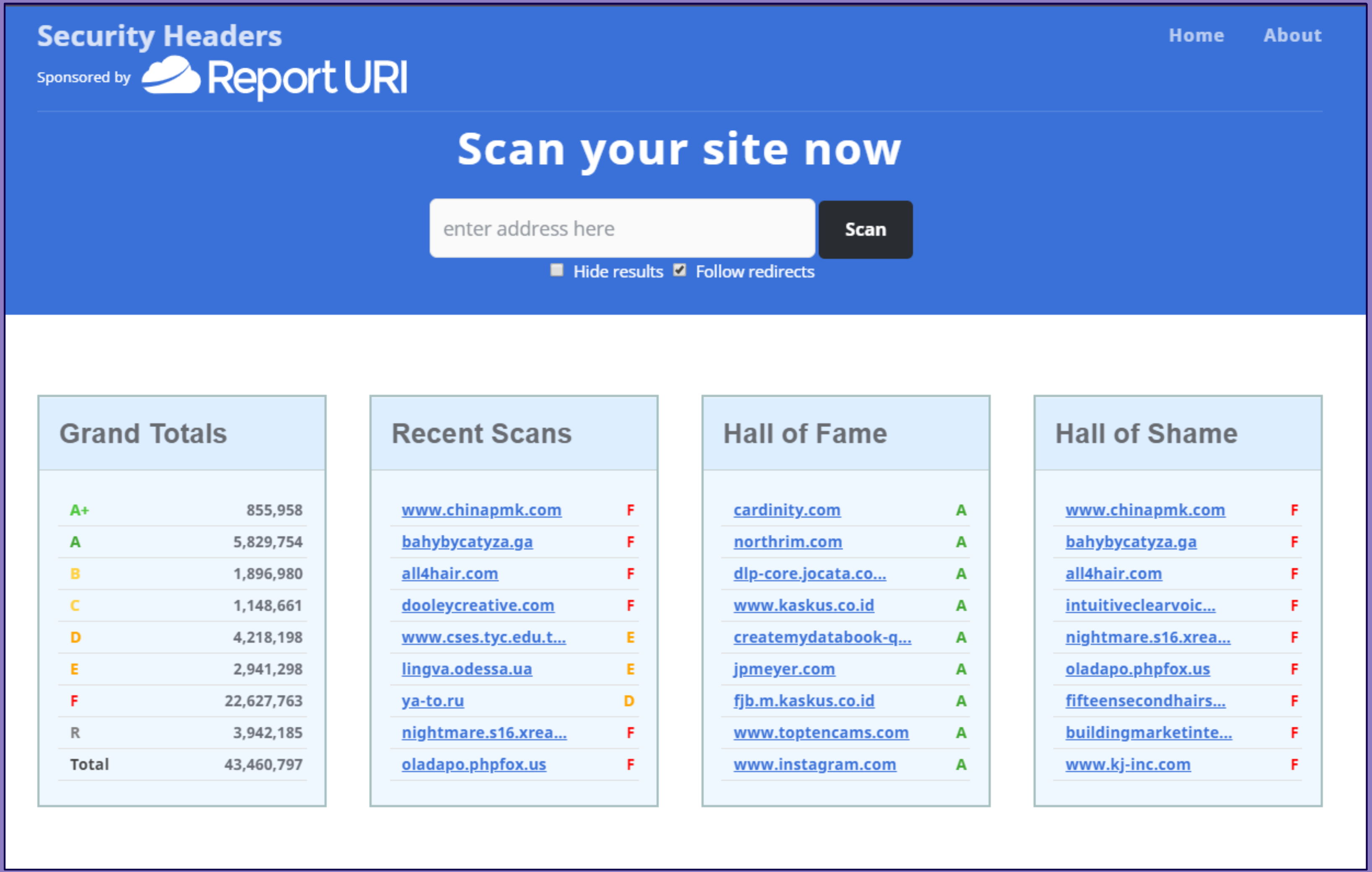
Photo source: Pixabay



The search engine that doesn't track you. Help Spread DuckDuckGo!

DuckDuckGo.com

HTTP Headers



Security Headers

Sponsored by Report URI

Home About

Scan your site now

enter address here | Scan

□ Hide results ☑ Follow redirects

Grand Totals

A+	855,958
A	5,829,754
B	1,896,980
C	1,148,661
D	4,218,198
E	2,941,298
F	22,627,763
R	3,942,185
Total	43,460,797

Recent Scans

www.chinapmk.com	F
bahybycatyza.ga	F
all4hair.com	F
dooleycreative.com	F
www.cses.tyc.edu.t...	E
lingva.odessa.ua	E
ya-to.ru	D
nightmare.s16.xrea...	F
oladapo.phpfox.us	F

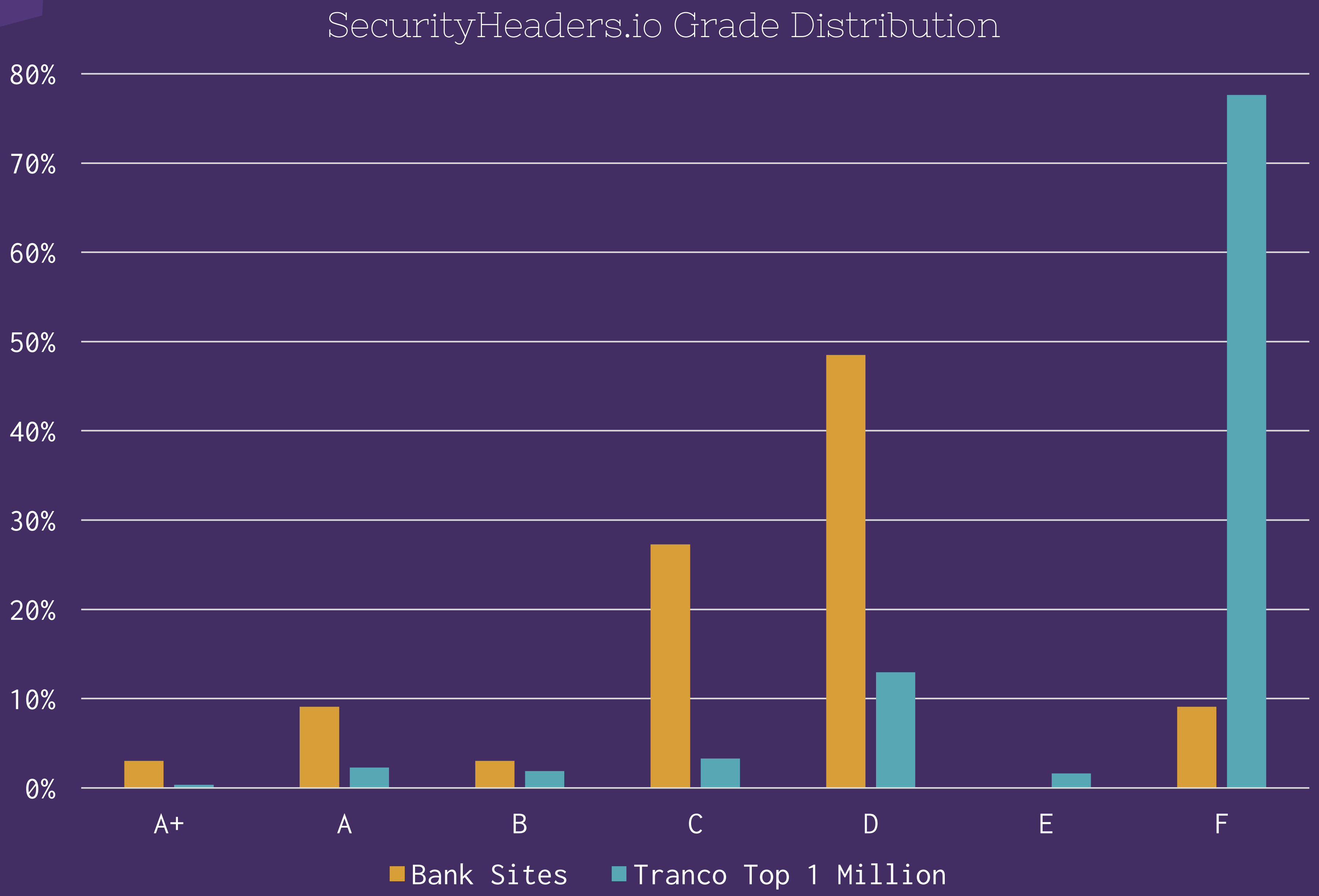
Hall of Fame

cardinity.com	A
northrim.com	A
dlp-core.jocata.co...	A
www.kaskus.co.id	A
createmydatabook-q...	A
jpmeyer.com	A
fjb.m.kaskus.co.id	A
www.toptencams.com	A
www.instagram.com	A

Hall of Shame

www.chinapmk.com	F
bahybycatyza.ga	F
all4hair.com	F
intuitiveclearvoic...	F
nightmare.s16.xrea...	F
oladapo.phpfox.us	F
fifteensecondhairs...	F
buildingmarketinte...	F
www.kj-inc.com	F

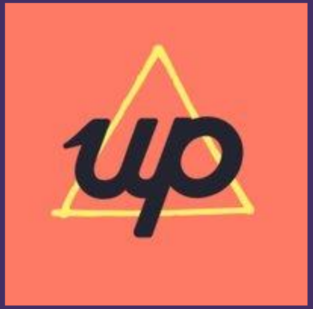
Securityheaders.com



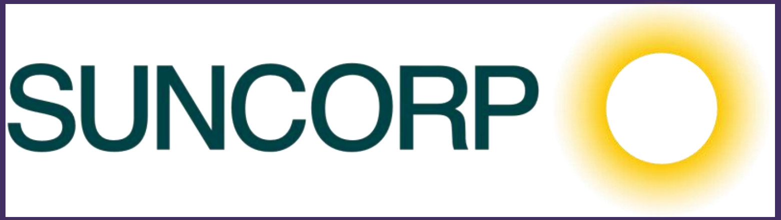
Top 1 Million Analysis - September 2019 - https://scotthelme.co.uk/ - 2019-10-03

How did they go?

Winner:



Runner Up:



Strict-Transport-Security

- Defends against PITM attacks
- Activated in browser if:
  - Connection is HTTPS with a valid certificate
  - Valid HSTS header sent
- Once activated:
  - HTTP links are converted to HTTPS
  - Disables click-through on Certificate warnings

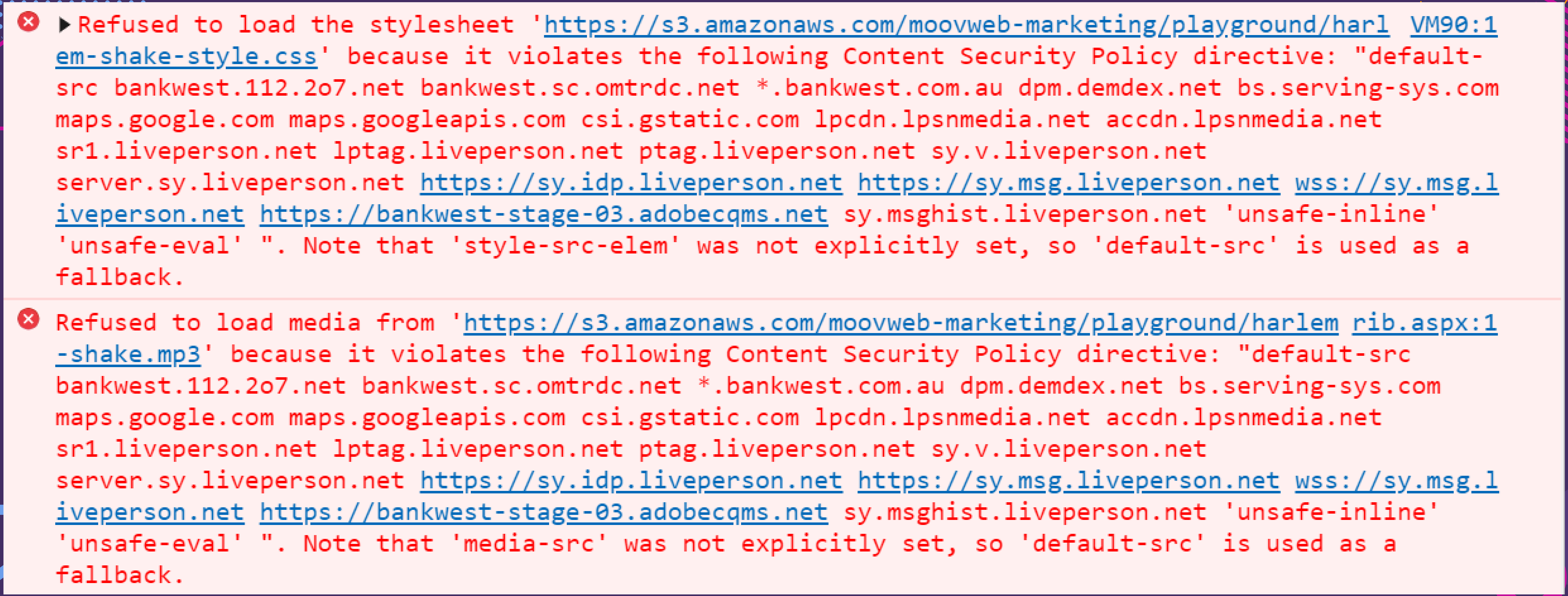
HSTS Preload

- A valid certificate
- Redirect HTTP > HTTPS
- Serve all subdomains over HTTPS
- Serve a HSTS header on the base domain
- Header must specify:
  - max-age of 1 year
  - includeSubDomains directive
  - preload directive
- Submit to hstspreload.org

Photo source: Pixabay

content-security-policy

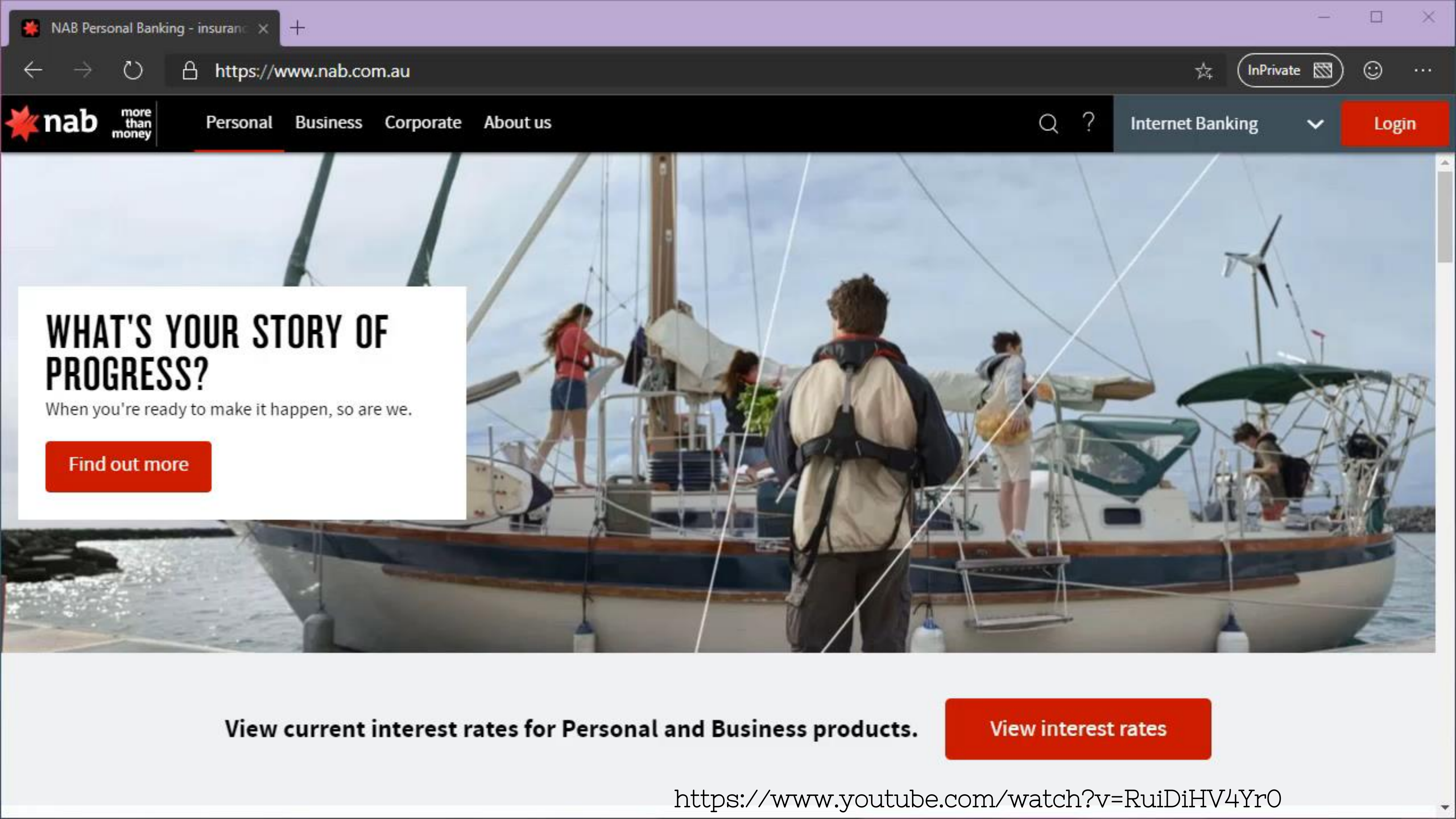
- Mitigates Cross Site Scripting (XSS) and data injection attacks
- Whitelist of resources that can be loaded
- Violations can be reported by browser
- Report only mode: content-security-policy-report-only



```
▶ Refused to load the stylesheet 'https://s3.amazonaws.com/moovweb-marketing/playground/harl  VM90:1
em-shake-style.css' because it violates the following Content Security Policy directive: "default-
src bankwest.112.2o7.net bankwest.sc.omtrdc.net *.bankwest.com.au dpm.demdex.net bs.serving-sys.com
maps.google.com maps.googleapis.com csi.gstatic.com lpcdn.lpsnmedia.net accdn.lpsnmedia.net
sr1.liveperson.net lptag.liveperson.net ptag.liveperson.net sy.v.liveperson.net
server.sy.liveperson.net https://sy.idp.liveperson.net https://sy.msg.liveperson.net wss://sy.msg.l
iveperson.net https://bankwest-stage-03.adobecqms.net sy.msghist.liveperson.net 'unsafe-inline'
'unsafe-eval' ". Note that 'style-src-elem' was not explicitly set, so 'default-src' is used as a
fallback.

Refused to load media from 'https://s3.amazonaws.com/moovweb-marketing/playground/harlem rib.aspx:1
-shake.mp3' because it violates the following Content Security Policy directive: "default-src
bankwest.112.2o7.net bankwest.sc.omtrdc.net *.bankwest.com.au dpm.demdex.net bs.serving-sys.com
maps.google.com maps.googleapis.com csi.gstatic.com lpcdn.lpsnmedia.net accdn.lpsnmedia.net
sr1.liveperson.net lptag.liveperson.net ptag.liveperson.net sy.v.liveperson.net
server.sy.liveperson.net https://sy.idp.liveperson.net https://sy.msg.liveperson.net wss://sy.msg.l
iveperson.net https://bankwest-stage-03.adobecqms.net sy.msghist.liveperson.net 'unsafe-inline'
'unsafe-eval' ". Note that 'media-src' was not explicitly set, so 'default-src' is used as a
fallback.
```

⚠ Warning ⚠



WHAT'S YOUR STORY OF PROGRESS?

When you're ready to make it happen, so are we.

View current interest rates for Personal and Business products.

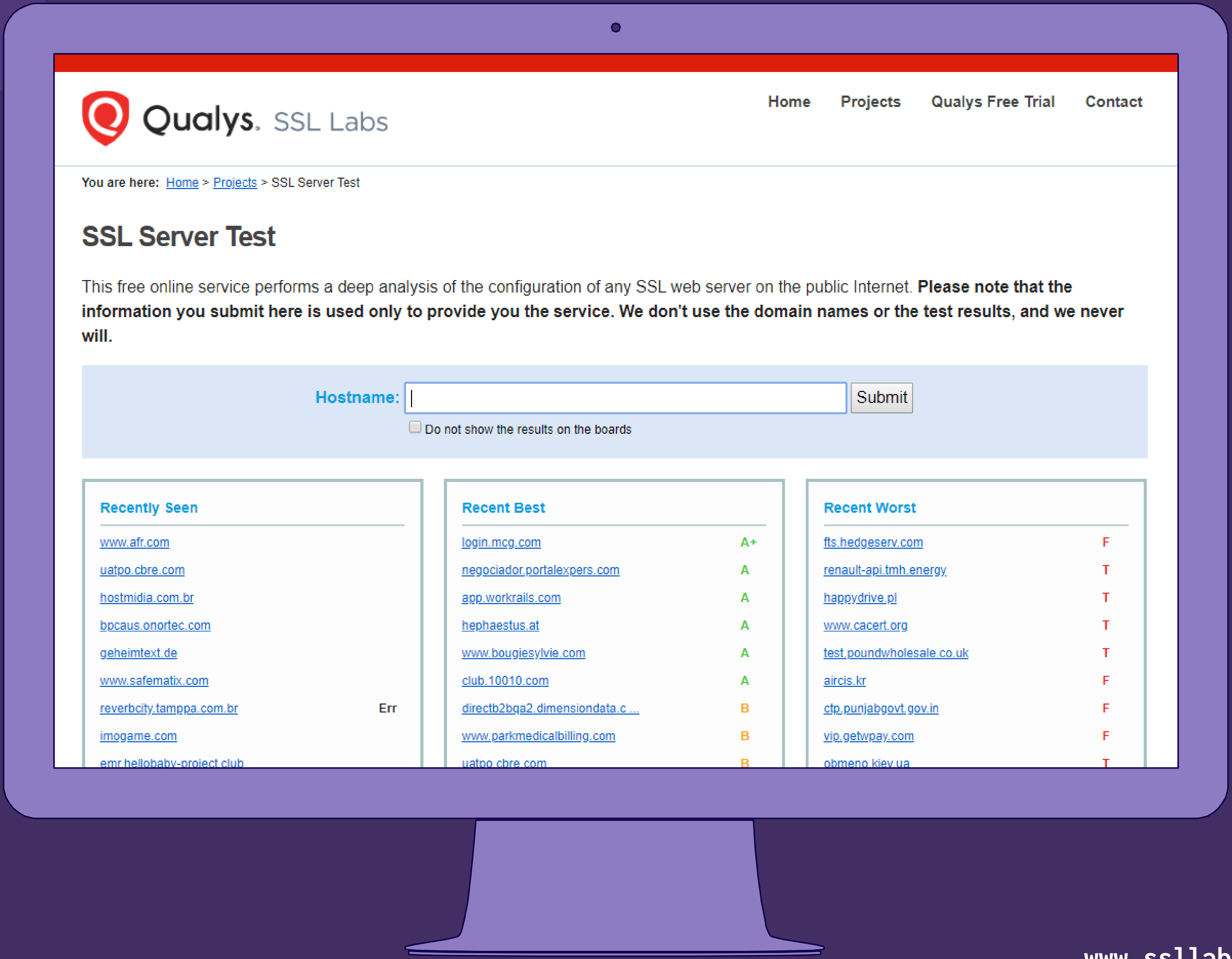
https://www.youtube.com/watch?v=RuiDiHV4Yr0

Photo source: Luis Quintero

What can you do?

- Review response headers
- Deploy security response headers
- Consider monitoring tools like report-uri.com

SSL/TLS Configuration



You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: | Submit

□ Do not show the results on the boards

Recently Seen

www.afr.com	
uatpo.cbre.com	
hostmidia.com.br	
bpcaus.onortec.com	
geheimtext.de	
www.safematix.com	
reverbcity.tamppa.com.br	Err
imogame.com	
emr.hellobaby-project.club	

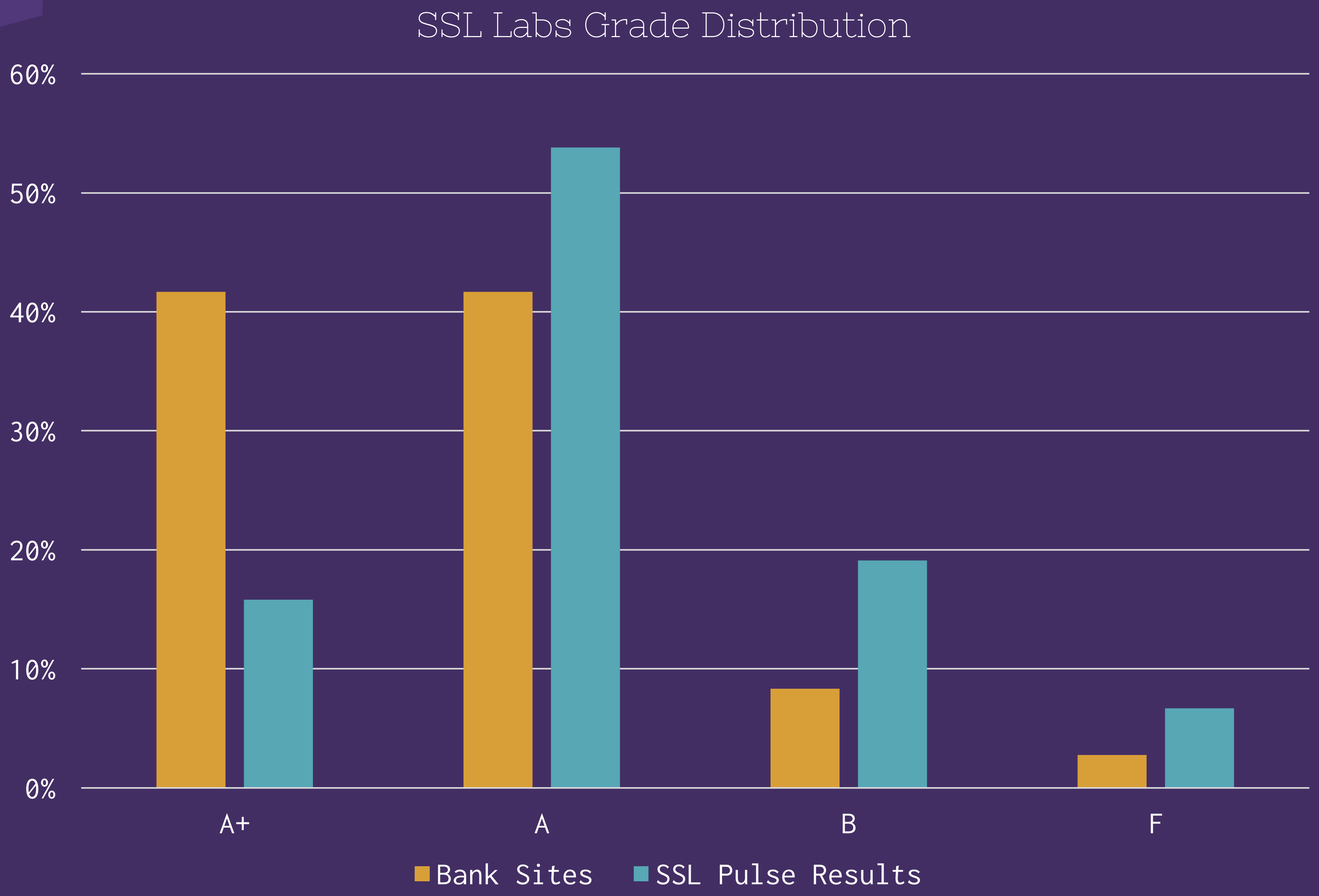
Recent Best

login.mcg.com	A+
negociador.portalexpers.com	A
app.workrails.com	A
hephaestus.at	A
www.bougiesylvie.com	A
club.10010.com	A
directb2bqa2.dimensiondata.c ...	B
www.parkmedicalbilling.com	B
uatpo.cbre.com	B

Recent Worst

fts.hedgeserv.com	F
renault-api.tmh.energy	T
happydrive.pl	T
www.cacert.org	T
test.poundwholesale.co.uk	T
aircis.kr	F
ctp.punjabgovt.gov.in	F
vip.getwpay.com	F
obmeno.kiev.ua	T

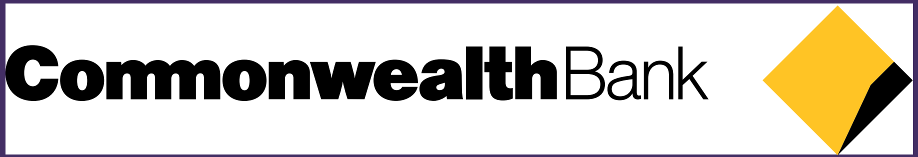
www.ssllabs.com

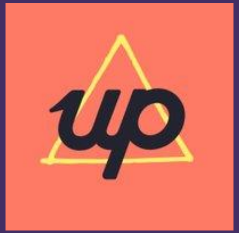


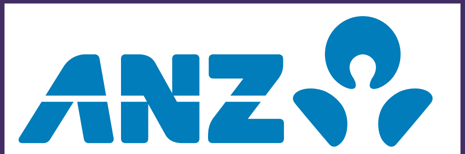
SSL Pulse - https://www.ssllabs.com/ssl-pulse/ - 2019-09-15

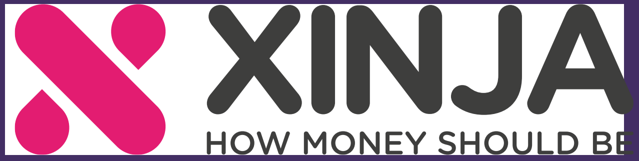
How Did They Go

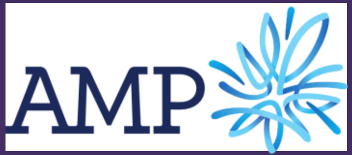
Winners:

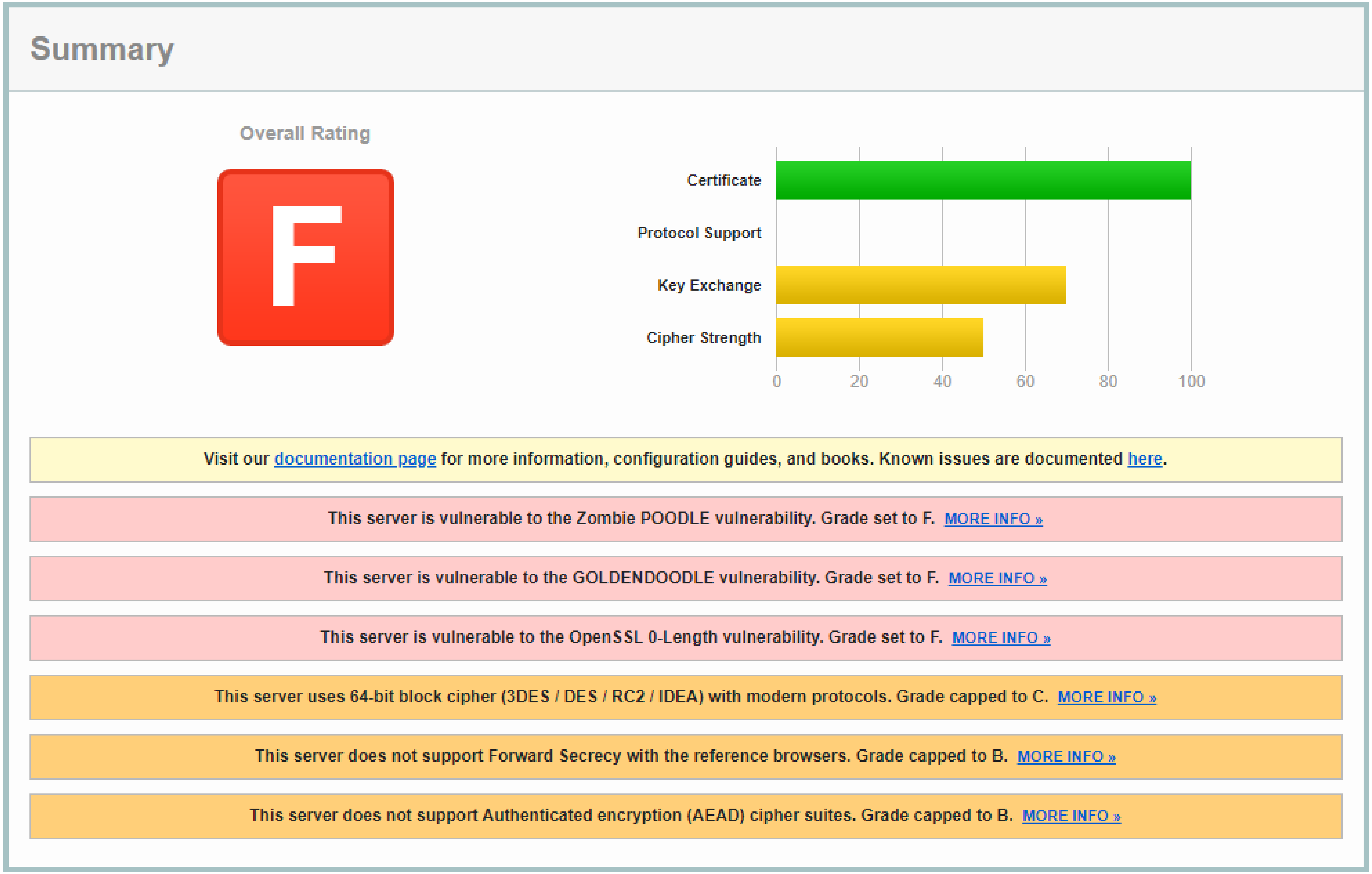












Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the Zombie POODLE vulnerability. Grade set to F. MORE INFO »

This server is vulnerable to the GOLDENDOODLE vulnerability. Grade set to F. MORE INFO »

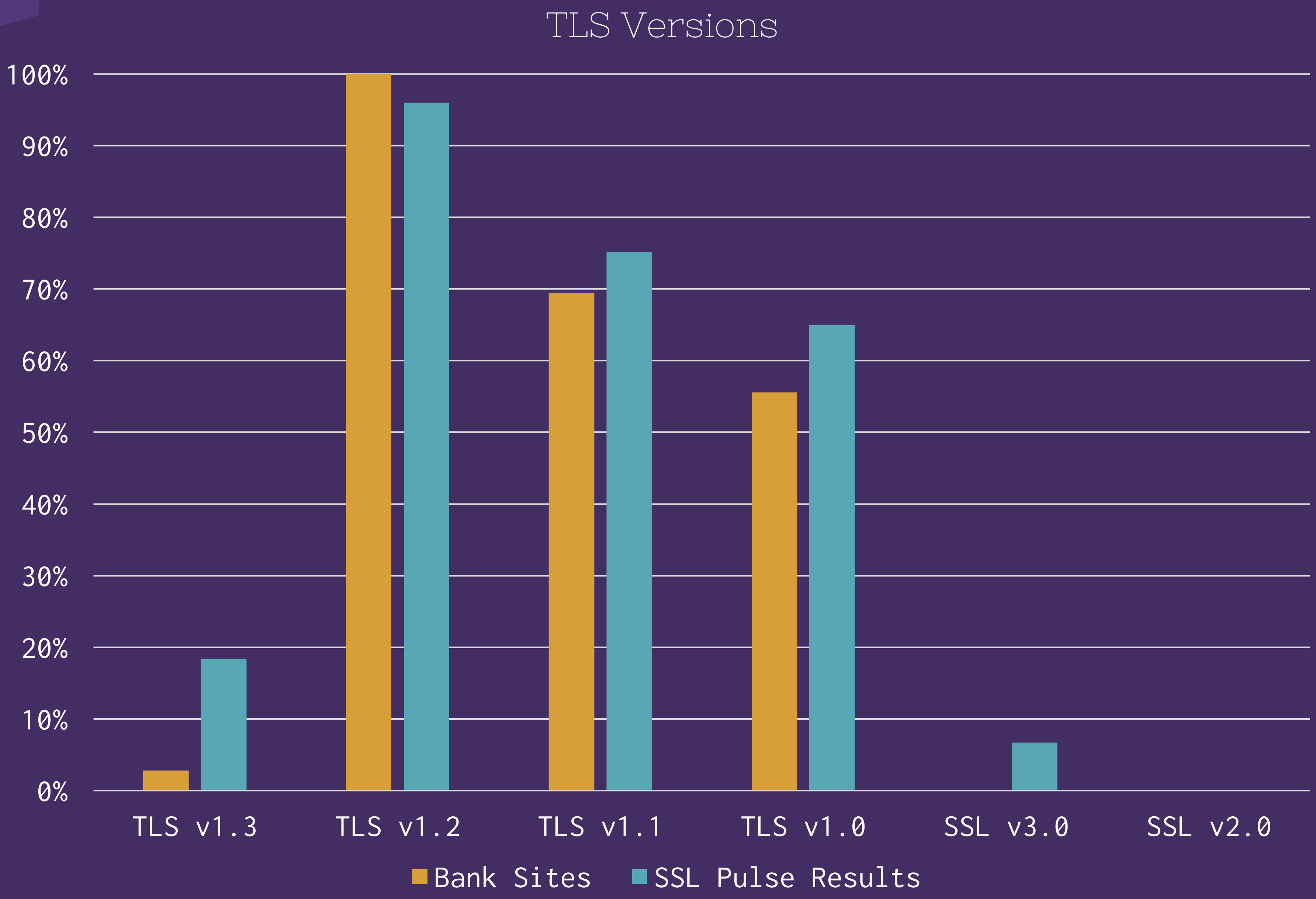
This server is vulnerable to the OpenSSL 0-Length vulnerability. Grade set to F. MORE INFO »

This server uses 64-bit block cipher (3DES / DES / RC2 / IDEA) with modern protocols. Grade capped to C. MORE INFO »

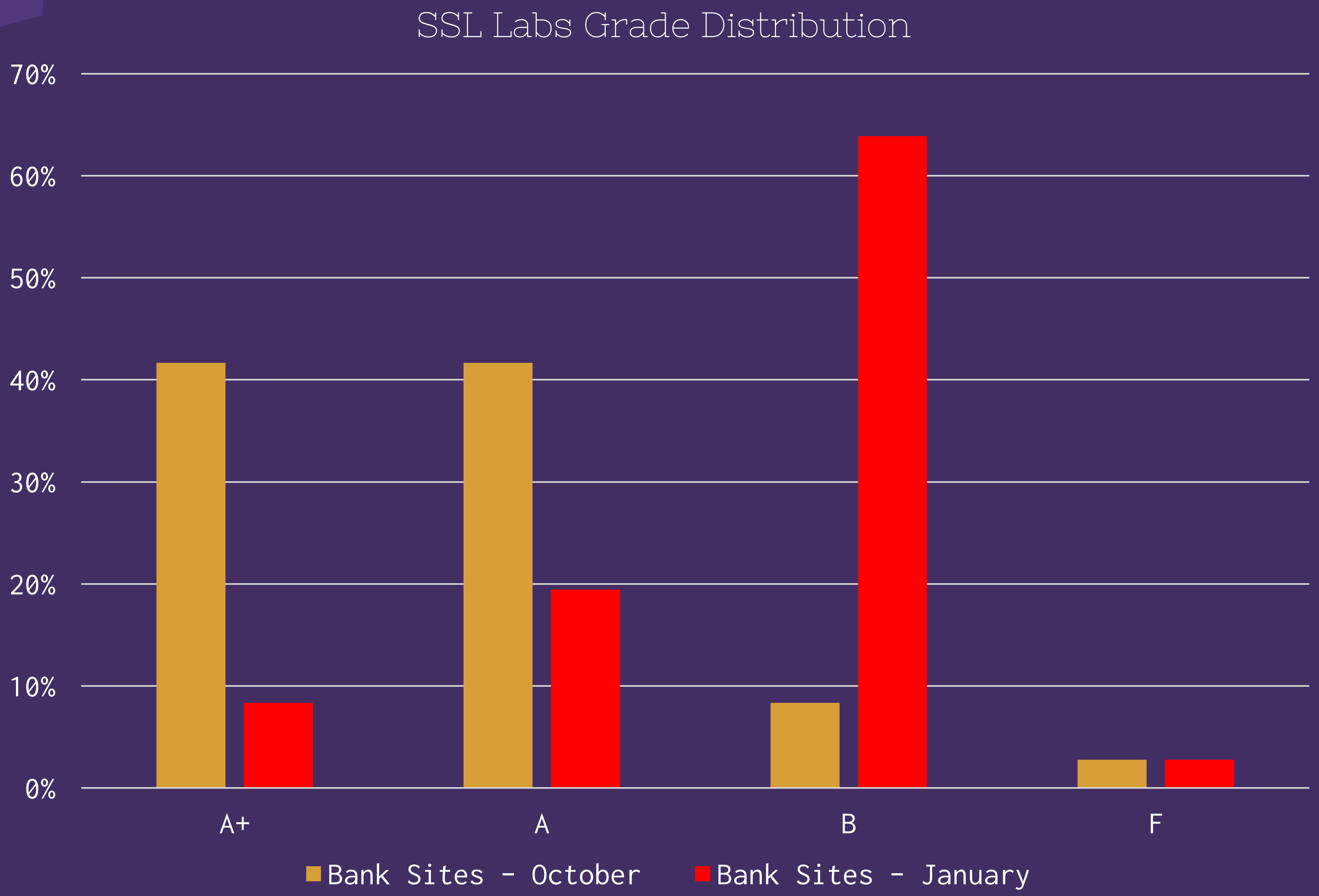
This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

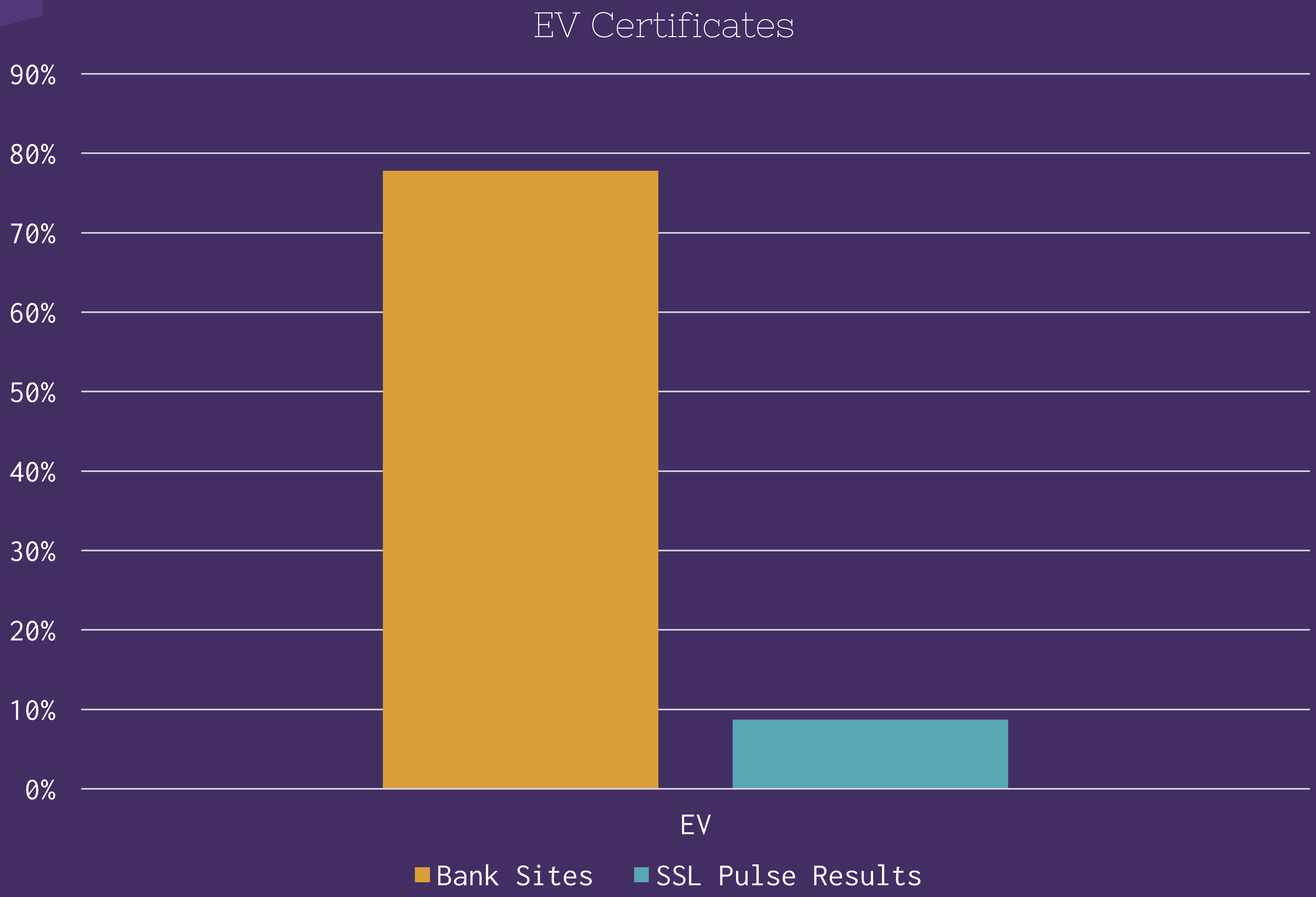
Photo source: Tropical.Pete on Flickr



SSL Pulse - https://www.ssllabs.com/ssl-pulse/ - 2019-09-15



SSL Pulse - https://www.ssllabs.com/ssl-pulse/ - 2019-09-15

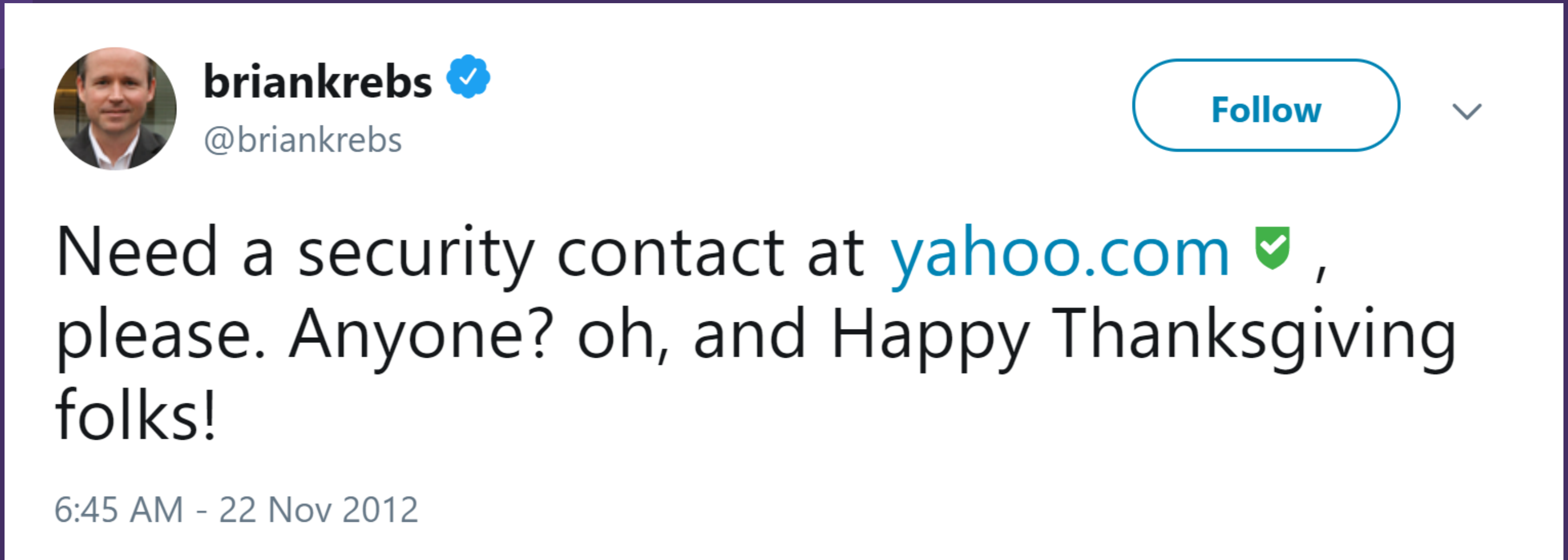


SSL Pulse - https://www.ssllabs.com/ssl-pulse/ - 2019-09-15

What can you do?

- Keep deploying TLS/SSL
- Follow best practice guides - https://bit.ly/2aSNEEg
- Use tools to monitor and validate your configuration

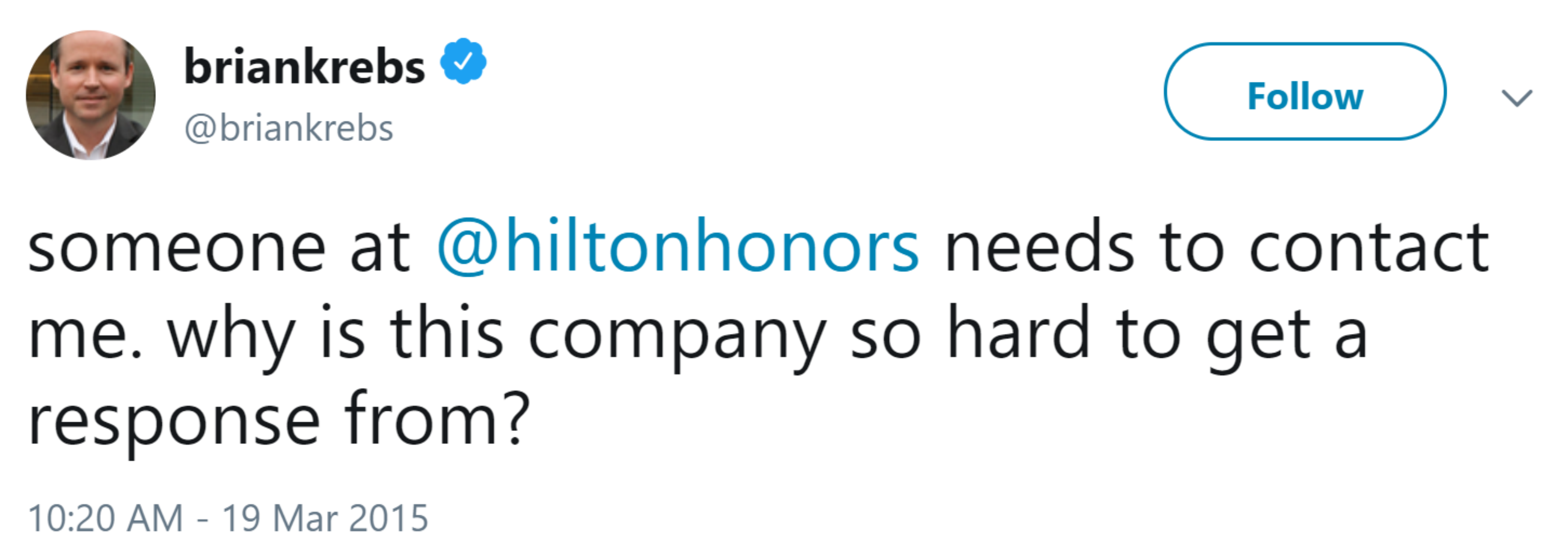
Security.txt



briankrebs
@briankrebs

Need a security contact at yahoo.com , please. Anyone? oh, and Happy Thanksgiving folks!

6:45 AM - 22 Nov 2012



briankrebs
@briankrebs

someone at @hiltonhonors needs to contact me. why is this company so hard to get a response from?

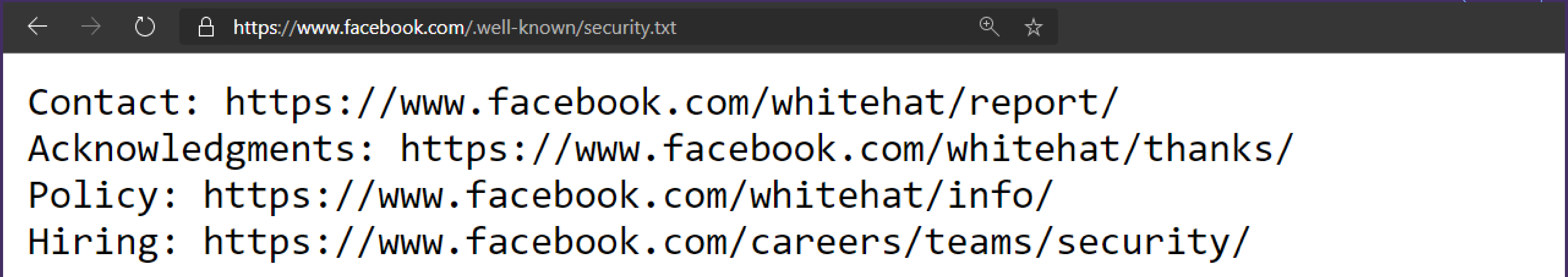
10:20 AM - 19 Mar 2015

Photo source: Marvel

What is security.txt?

- <domain>/.well-known/security.txt
- Proposed IEFT standard
- Helps define the process for people to disclose security vulnerabilities
- Specify:

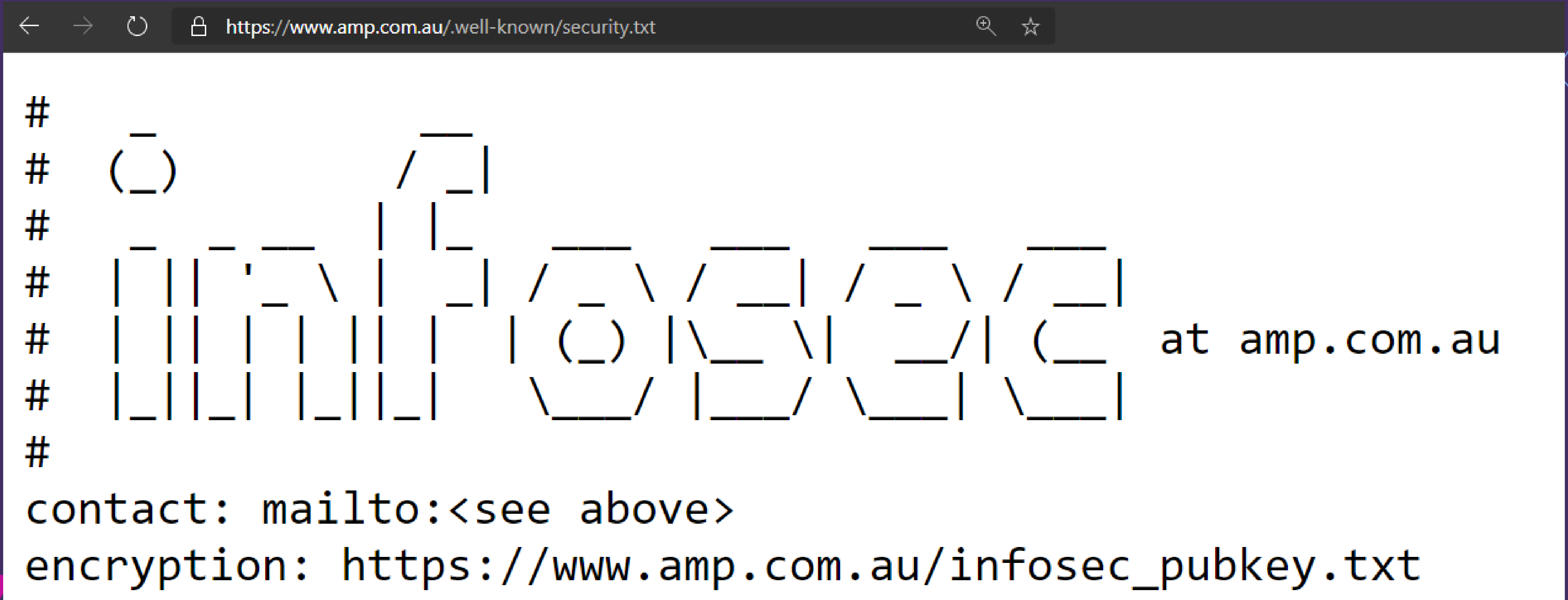
  contact, encryption, acknowledgements, preferred languages, policies and hiring links



https://www.facebook.com/.well-known/security.txt

```
Contact: https://www.facebook.com/whitehat/report/
Acknowledgments: https://www.facebook.com/whitehat/thanks/
Policy: https://www.facebook.com/whitehat/info/
Hiring: https://www.facebook.com/careers/teams/security/
```

How did the Banks go?



https://www.amp.com.au/.well-known/security.txt

```
#   _          __
#  (_)        / _|
#   _  _ __  | |_   ___   ___   ___   ___
#  | || '_ \ |  _| / _ \ / __| / _ \ / __|
#  | || | | || |  | (_) |\__ \|  __/| (__  at amp.com.au
#  |_||_| |_||_|   \___/ |___/ \___| \___|
#
contact: mailto:<see above>
encryption: https://www.amp.com.au/infosec_pubkey.txt
```

What can you do?

- Go to securitytxt.org and generate a file
- Contact directive is mandatory
- Encryption directive is recommended
- It is recommended that you digitally sign the file

What else could we have looked at?

- Email - SPF, DKIM, DMARC
- DNS - CAA, DNSSEC
- MFA
- Password Requirements
- Reported Breaches

Photo source: American Zoetrope, Columbia

Photo source: Warner Bros

Resources

- Securityheaders.com
- Harlem Shake - https://pastebin.com/aJna4paJ
- Ssllabs.com
- SSL Best Practices -https://bit.ly/2aSNEEg
- Hardenize.com
- Hstspreload.org
- Securitytxt.org

Thanks!

You can find me at @kjacobsen & https://poshsecurity.com