nic.br cgi.br | cert.br

***Workshop* CKN**

07 de dezembro de 2021

Evento *Online*

TLP:WHITE

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e Político

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial, coordenada pelo MCTI
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Padrões Modernos para Segurança e Estabilidade dos Serviços

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br nic.br cgi.br

Todos Tem um Papel na Segurança:
Ecossistema é Complexo e Interdependente

TLP:WHITE

Quase tudo é *software* e está conectado à Internet

Ataques são constantes

- Motivações diversas
- Volume crescente
  - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

Melhora do cenário depende de cada ator fazer sua parte

TLP:WHITE

Precisamos Cuidar da Base Primeiro:
Causas Mais Comuns de Invasões e Vazamentos de Dados

Ataques mais reportados e mais observados em sensores do CERT.br:

- Tentativas de fraudes financeiras e de comércio eletrônico
  - via e-mails falsos (***phishings***)
  - via infecção de roteadores de banda larga (CPEs) para **DNS *hijacking***
  - via infecção de computadores e de celulares
- Invasão por meio de **senhas comprometidas**, vazadas ou fracas
  - via ***phishing***
  - via força bruta
  - senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas

  Exemplos de serviços afetados:
  - *e-mails* e serviços em nuvem
  - acesso remoto (VPN, SSH, RDP, Winbox, etc)
  - gestão remota de ativos de rede e servidores
- Exploração de vulnerabilidades para invasão e/ou movimentação lateral
  - falta de aplicação de correções
  - **erros de configuração**
  - **falta / falha de processos**

Veja também: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse **mais atenção a erros e configurações**
- todos os serviços tivessem 2FA / MFA

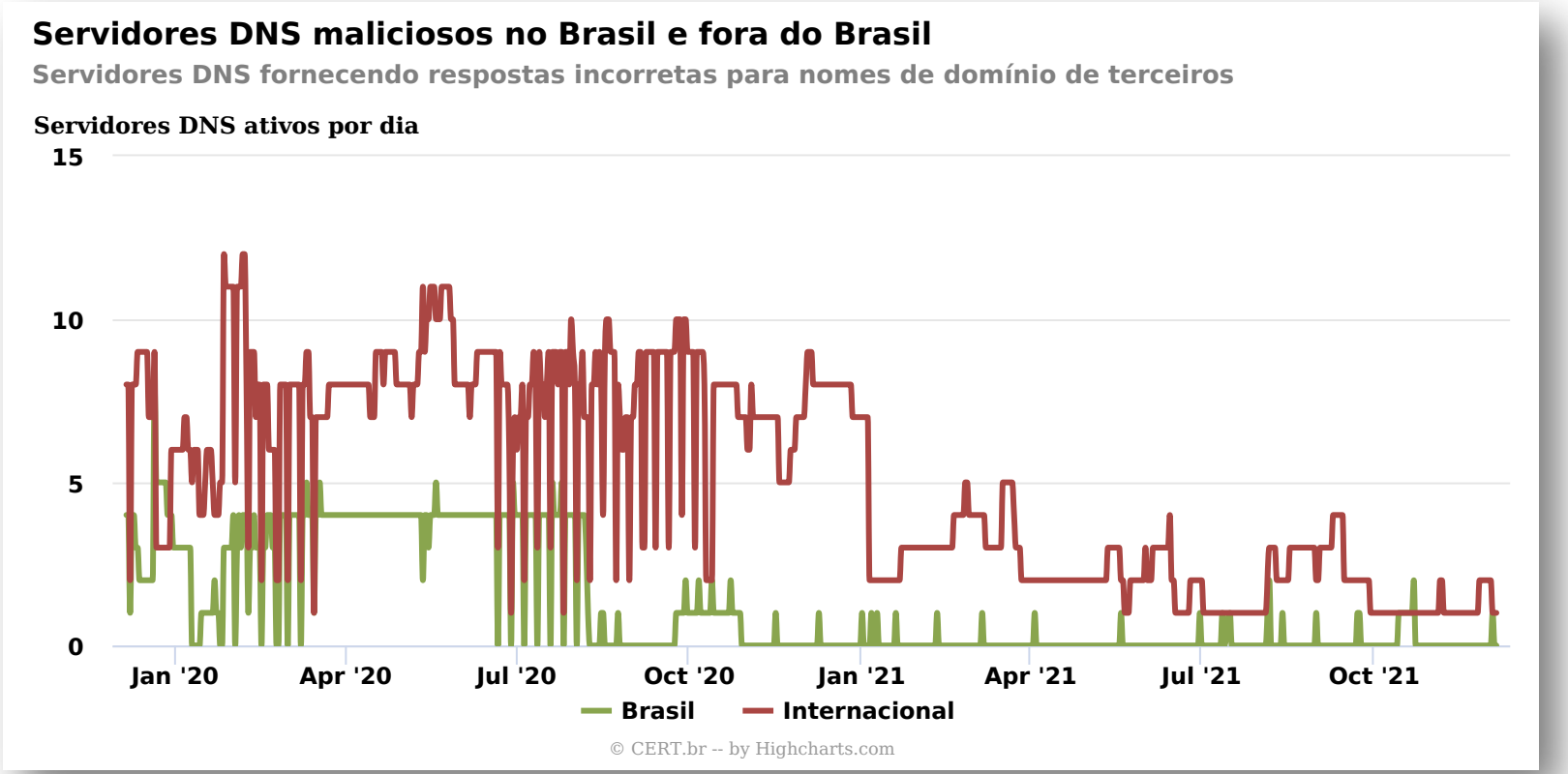
Estudo Setorial Segurança digital: uma análise de gestão de risco em empresas brasileiras
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Servidores DNS Maliciosos Usados nos CPEs Invadidos: **Fornecem Respostas Autoritativas Erradas**

TLP:WHITE

Domínios afetados dos seguintes setores:

- Bancos, Serviços de Pagamento, Serviços de *Streaming*, Mobilidade, Redes Sociais, *Webmail*, Comércio Eletrônico, entre outros



Fonte: https://cert.br/stats/dns-malicioso/

Semântica é importante ao reportar incidentes ou pedir takedown!

- **Isto não é um DNS invadido**
- **Isto não é envenenamento (*cache poisoning*)**
- **Isto não é sequestro de domínio (*domain hijacking*)**

Isto é um servidor DNS malicioso (*rogue*) sendo usado para sequestro de DNS (*DNS hijacking*)

- **autoritativo para os domínios das vítimas**
- **recursivo aberto respondendo ao restante das consultas**

TLP:WHITE

Padrões Modernos que Aumentam a Segurança

	Padrões	Vantagens da Adoção
Autenticação com Múltiplos Fatores	Tokens • em *hardware* (FIDO2/U2F) • em *software* (HOTP/TOTP)	Impede sucesso de força bruta de senhas Reduz impacto do comprometimento de credenciais
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de *cache* Habilitar o uso de outras tecnologias como o DANE
Segurança de *e-mail*	STARTTLS • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra *sniffing* (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir *phishing* da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou • novas redes só terão IPv6 • redes móveis já tem IPv6 nativo	Mais estabilidade e menor complexidade • Não depender de CGN ou tradução v6 → v4 • Não depender de transição, reduz superfície de ataques Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

TESTE OS PADRÕES

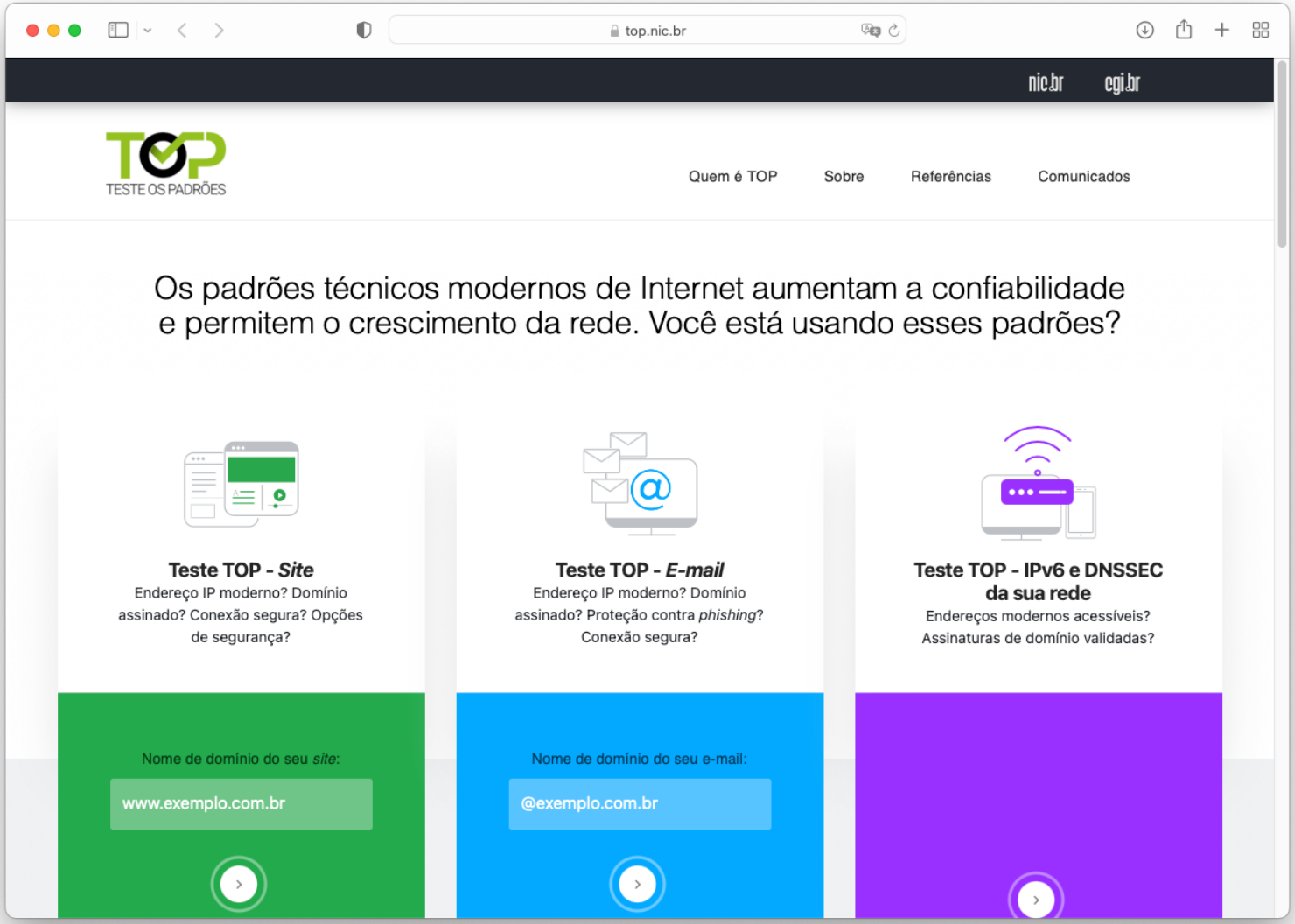
https://top.nic.br/
Padrões Testados

TLP:WHITE

	Padrões	Vantagens da Adoção
Autenticação com Múltiplos Fatores	Tokens • em *hardware* (FIDO2/U2F) • em *software* (HOTP/TOTP)	Impede sucesso de força bruta de senhas Reduz impacto do comprometimento de credenciais
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de *cache* Habilitar o uso de outras tecnologias como o DANE
Segurança de *e-mail*	STARTTLS • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra *sniffing* (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir *phishing* da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou • novas redes só terão IPv6 • redes móveis já tem IPv6 nativo	Mais estabilidade e menor complexidade • Não depender de CGN ou tradução v6 → v4 • Não depender de transição, reduz superfície de ataques Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

TLP:WHITE

https://top.nic.br/
Testes para *site*, *e-mail* e conectividade



Testes

- verificam a correta implementação dos padrões
- baseiam-se
  - nas especificações das RFCs
  - em padrões técnicos operacionais recomendados por entidades internacionais

Relatório

- detalhamento de todos os resultados
  - referências detalhadas dos padrões
  - indicações sobre como corrigir possíveis problemas

Apoiadores

conexis brasil.digital · REDETELESUL · abranet · abrint · AbraHosting · TelComp

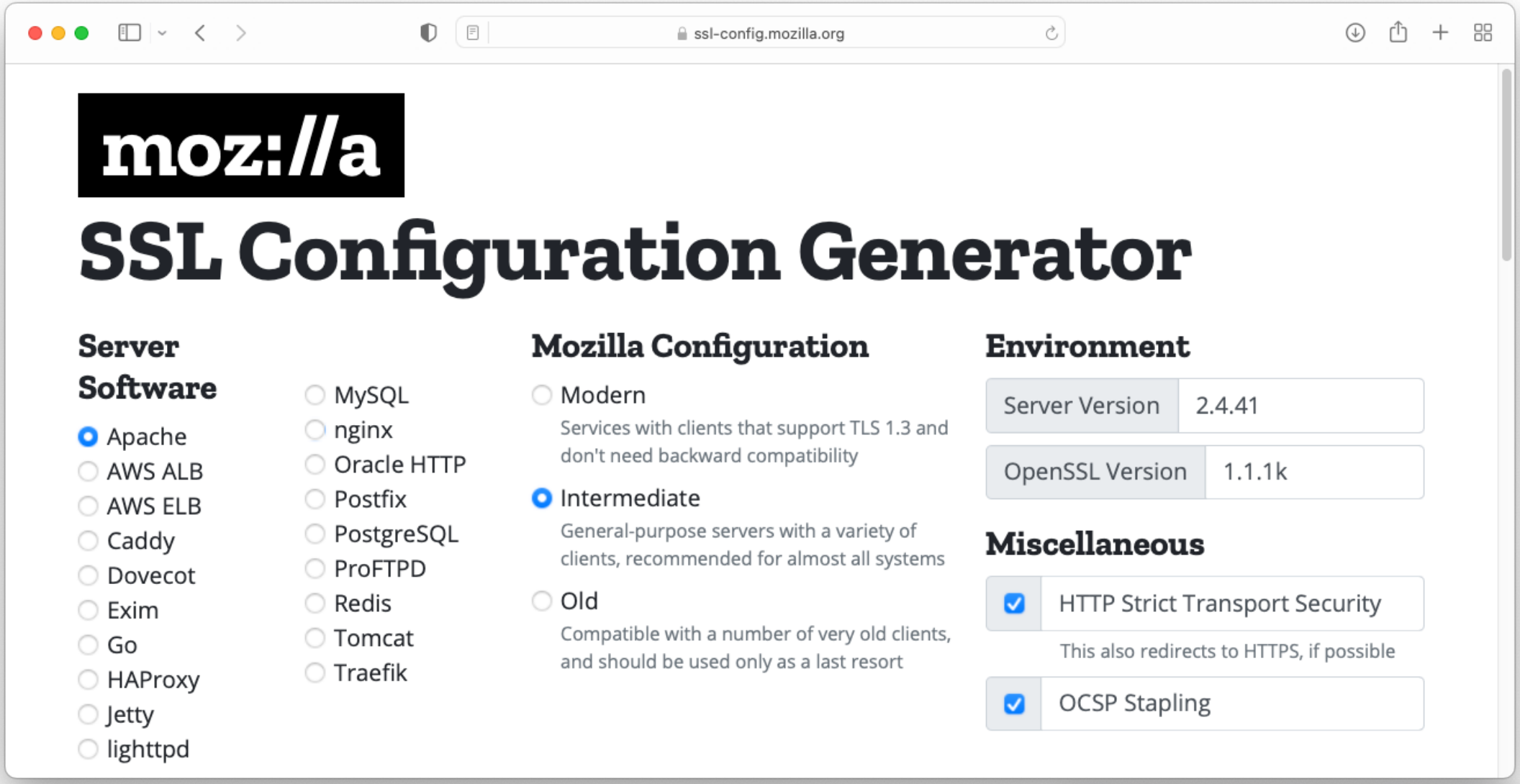
Outros *Sites* para Auxiliar nos Testes e Configurações

cert.br nic.br cgi.br

SSL Configuration Generator

https://ssl-config.mozilla.org/

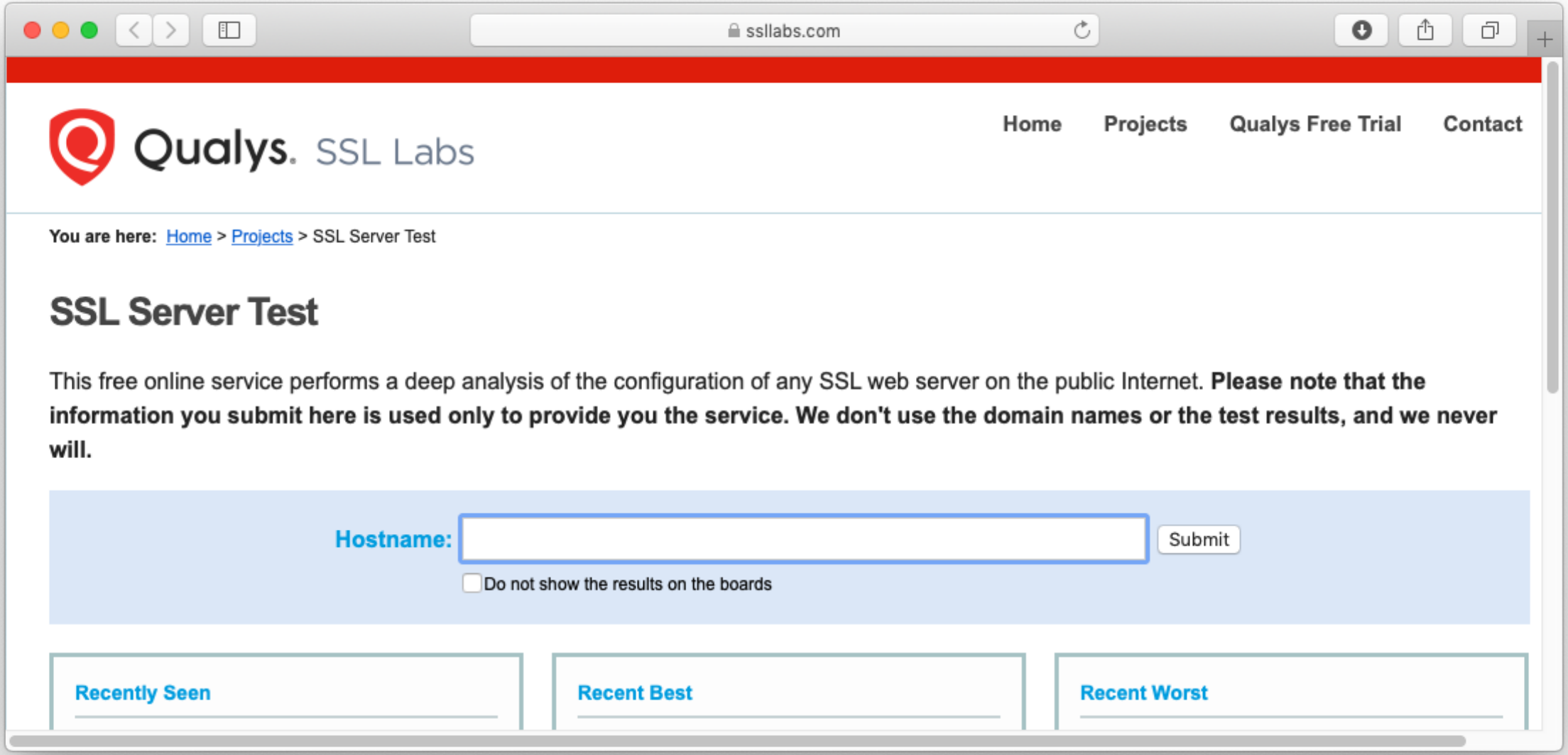
TLP:WHITE



SSL Server Test

https://www.ssllabs.com/ssltest/

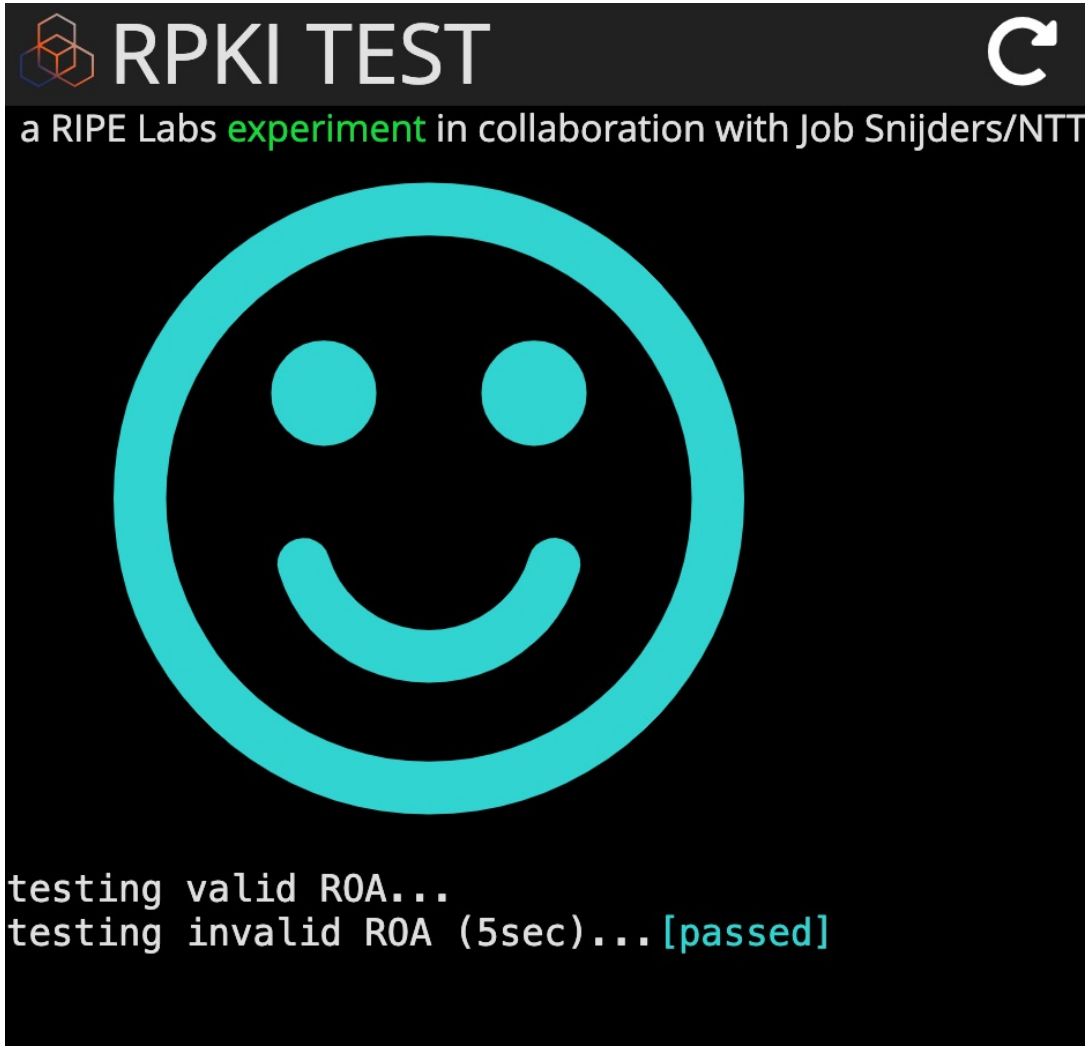
TLP:WHITE



RPKI TEST – A RIPE Labs experiment

https://sg-pub.ripe.net/jasper/rpki-web-test/

TLP:WHITE



TLP:WHITE

Referências dos Padrões Citados

Padrões	Referências
Tokens em *hardware* (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em *software* (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://mecsa.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com
RPKI	https://bcp.nic.br/rpki https://sg-pub.ripe.net/jasper/rpki-web-test/

Outras Iniciativas para uma Internet mais Segura

cert.br nic.br cgi.br

Precisamos um Ecossistema mais Saudável: **Programa por uma Internet mais Segura**

TLP:WHITE

PROGRAMA INTERNET +SEGURA

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee

https://bcp.nic.br/i+seg

Conscientização:
Portal InternetSegura.br

TLP:WHITE

TLP:WHITE

Cartilha de Segurança para Internet: **Fascículos e *Slides* para Palestras e Treinamento**

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet
- ***Slides*** sobre cada um dos temas, que podem ser utilizados, por exemplo, para dar aulas ou palestras de conscientização
  - Dica do dia no *site*, via *Twitter* e RSS
  - Impressões em pequena escala enviadas a escolas e centros de inclusão digital
  - Possível gerar versões personalizadas com logo da instituição

    Exemplos de parceiros de impressão e distribuição:

    Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP

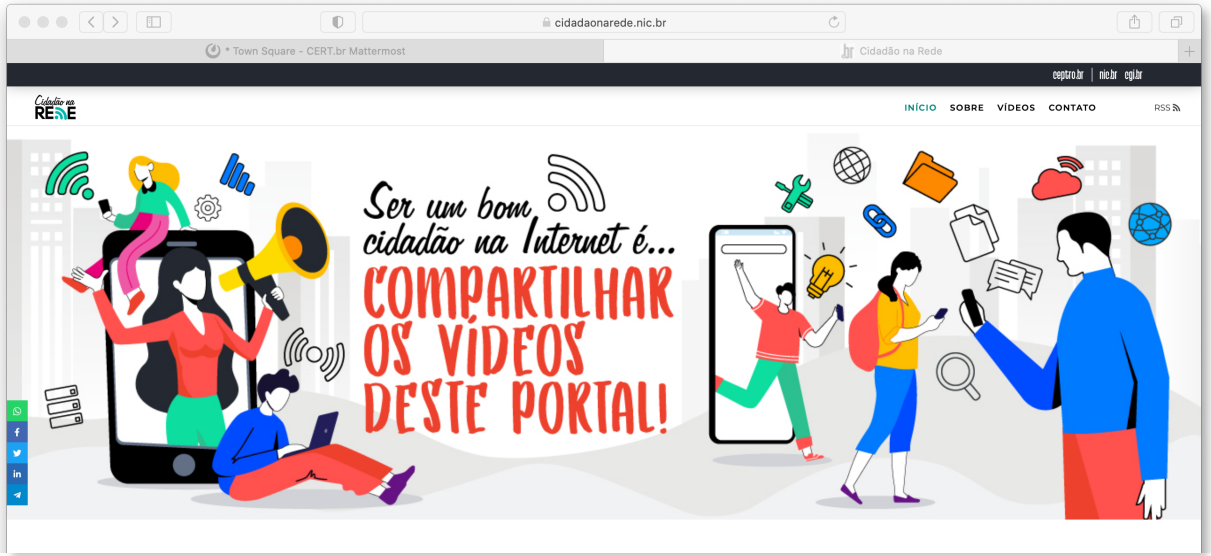
https://cartilha.cert.br/

TLP:WHITE

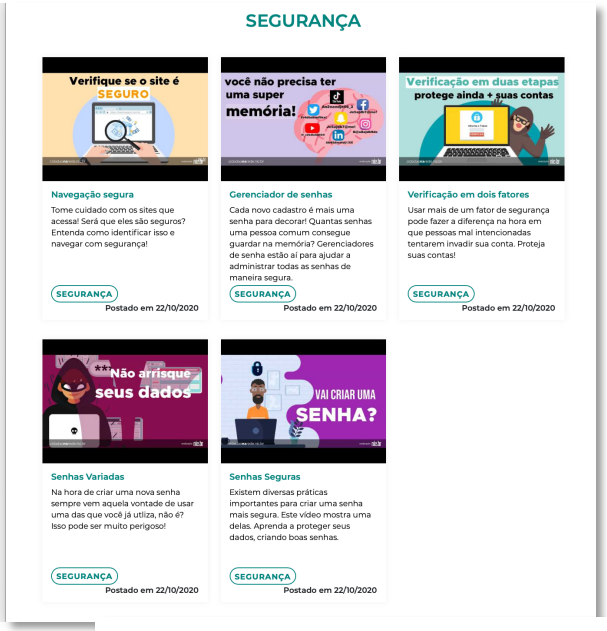
Projeto Cidadão na Rede

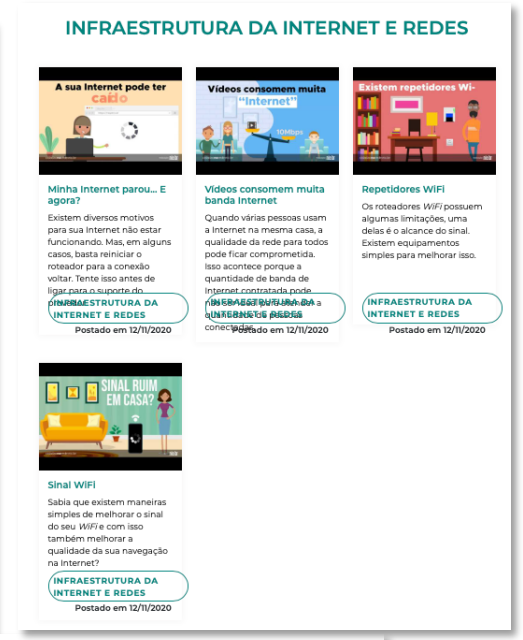
“É direito e dever de cada pessoa ser um bom cidadão, e isso também vale para o mundo digital, usando de forma responsável as Tecnologias de Informação e Comunicação, em particular a Internet.”

- Conduzido pelo Ceptro.br
- Vídeos curtos sobre diversos temas:
  - Segurança
  - Infraestrutura da Internet e redes
  - Uso responsável e deveres na Internet



https://cidadaonarede.nic.br/





Obrigado

cristine@cert.br jessen@cert.br

notificações para: cert@cert.br @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br