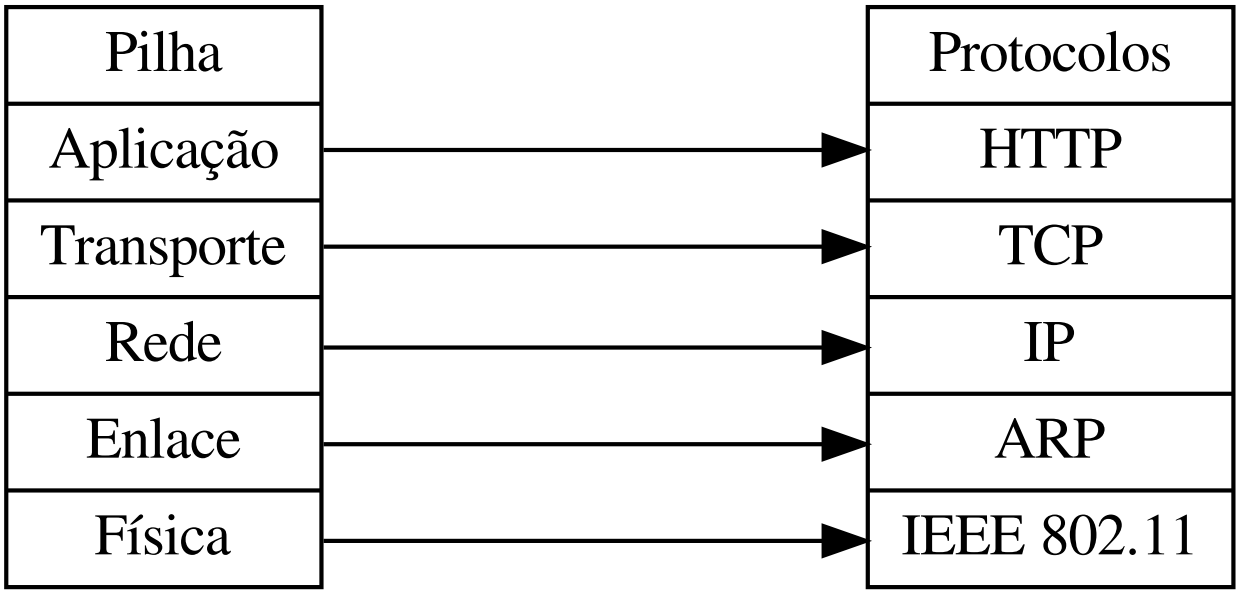
Segurança em redes

exemplos de exploits comuns e como lidar com elas

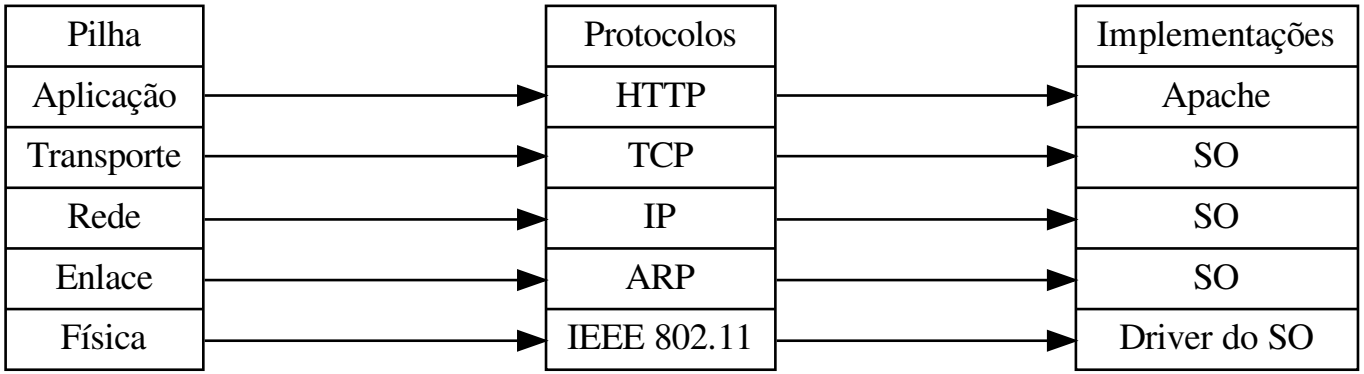
Giuliano Oliveira de Macedo

Modelo de software TCP/IP

Modelo de software TCP/IP



Modelo de software TCP/IP



CVE

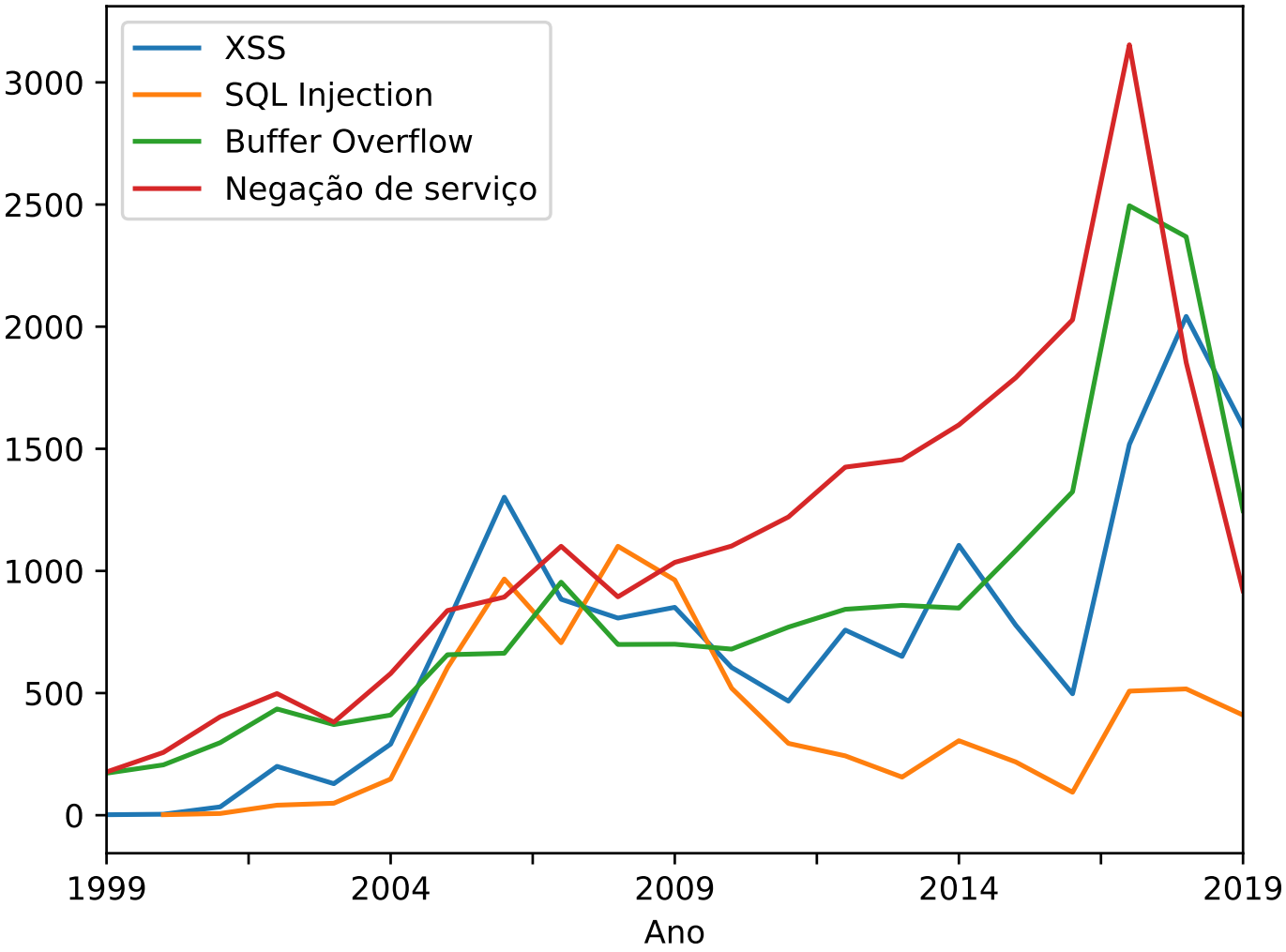
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-1020019	79		XSS	2019-07-29	2019-07-31	4.3	None	Remote	Medium	Not required	None	Partial	None
invenio-previewer before 1.0.0a12 allows XSS.														
2	CVE-2019-1020018	20			2019-07-29	2019-10-09	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Discourse before 2.3.0 and 2.4.x before 2.4.0.beta3 lacks a confirmation screen when logging in via an email link.														
3	CVE-2019-1020017	284			2019-07-29	2019-10-09	5.0	None	Remote	Low	Not required	None	Partial	None
Discourse before 2.3.0 and 2.4.x before 2.4.0.beta3 lacks a confirmation screen when logging in via a user-api OTP.														
4	CVE-2019-1020016	601			2019-07-29	2019-08-01	5.8	None	Remote	Medium	Not required	Partial	Partial	None
ASH-AIO before 2.0.0.3 allows an open redirect.														
5	CVE-2019-1020015	20			2019-07-29	2019-08-05	5.0	None	Remote	Low	Not required	None	Partial	None
graphql-engine (aka Hasura GraphQL Engine) before 1.0.0-beta.3 mishandles the audience check while verifying JWT.														
6	CVE-2019-1020014	415			2019-07-29	2019-08-19	2.1	None	Local	Low	Not required	Partial	None	None
docker-credential-helpers before 0.6.3 has a double free in the List functions.														
7	CVE-2019-1020013	287			2019-07-29	2019-08-01	5.0	None	Remote	Low	Not required	Partial	None	None
parse-server before 3.6.0 allows account enumeration.														
8	CVE-2019-1020012	444			2019-07-29	2019-08-02	5.0	None	Remote	Low	Not required	None	None	Partial
parse-server before 3.4.1 allows DoS after any POST to a volatile class.														
9	CVE-2019-1020011	20			2019-07-29	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
SmokeDetector intentionally does automatic deployments of updated copies of SmokeDetector without server operator authority.														

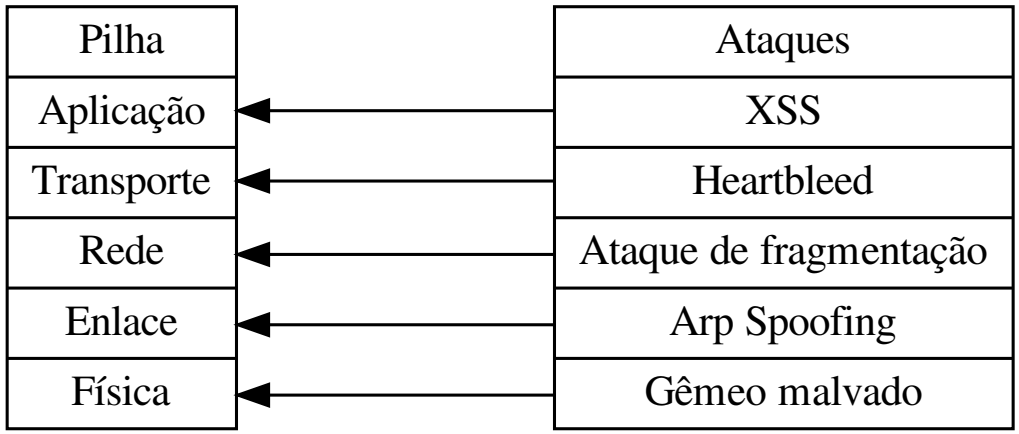
Termos comuns

- Vulnerabilidade
  - Qualquer falha ou brecha no algoritmo
- Exploit
  - Implementação real de uma vulnerabilidade
- Exemplo de vulnerabilidades
  - Buffer overlfow
  - DoS
  - Execução de código
  - Sql Injection
  - XSS
  - Bypassing
  - Ganhar informações
  - Elevar privilégio
  - etc

Ataques comuns ao longo dos anos 1999-2019



Exemplos de ataques e correspondência com o modelo de redes de 5 camadas



Exploits que irei mostrar

- XSS (Cross server scripting)
- ARP Spoofing (Manipulação de servidores/clientes ARP com o fim de espionagem)

Exemplo

Mitigação

Problemas:

1. O usuário deve ter o poder de ainda estilizar o texto
2. Tags de injeção de JS devem ser ignoradas

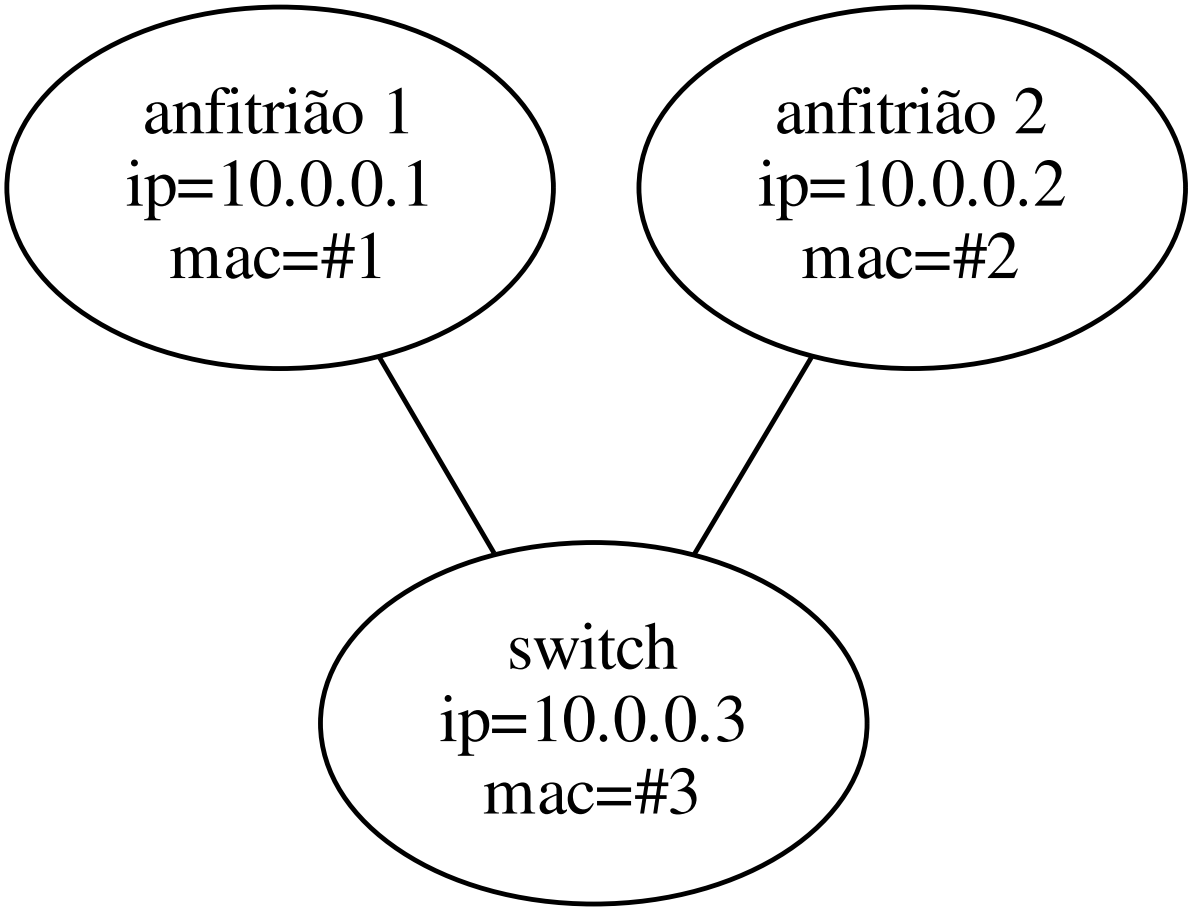
Minha solução

Solução para o problema 1
(O usuário deve ter o poder de ainda estilizar o texto)
Usar outra linguagem de marcação de texto como o **Markdown**

Minha solução

Solução para o problema 2
(Tags de injeção de JS devem ser ignoradas)
Limitar entrada do usuário:
Apenas os caracteres alfanuméricos com acento, números, os caracteres # e * serão aceitos

Exemplo


anfitrião 1
ip=10.0.0.1
mac=#1
anfitrião 2
ip=10.0.0.2
mac=#2
switch
ip=10.0.0.3
mac=#3

ARP Spoofing

site HTTP não seguro de propósito:
`http://testing-ground.scraping.pro/login`

Mitigação

Softwares de defesa :

- Agnitum Outpost Firewall
- AntiARP
- Antidote
- Arp_Antidote
- Arpalert
- Etc

Outra solução
HTTPS

Referências

- *Cve*, https://cve.mitre.org/.
- *Estastísticas de vulnerabilidades*, https://cve.mitre.org/.
- *Mitigação de xss*, https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html/.
- *Xss*, https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)/.

Obrigado

Código fonte dos exploits e desse slide estão disponíveis no repositório github:
`https://github.com/llpinokio/rc2t2`