

Segurança em redes

exemplos de exploits comuns e como lidar com elas

Giuliano Oliveira de Macedo

Modelo de software TCP/IP

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências



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.														

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

Ataques comuns ao longo dos anos 1999-2019

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

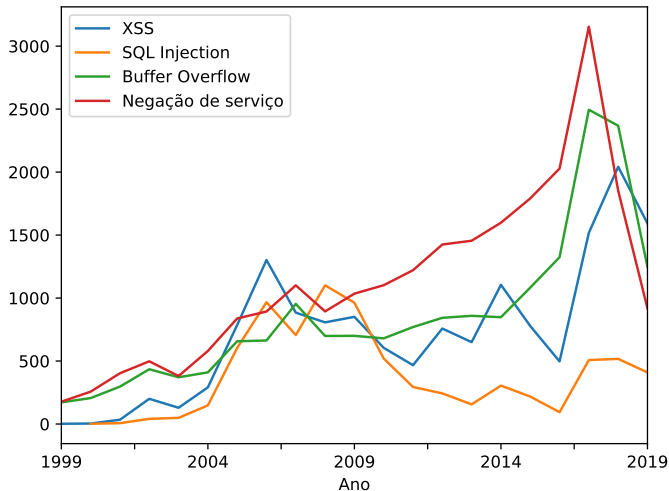
Contextualização

Ataques

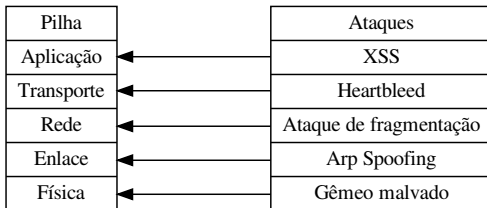
XSS

ARP Spoofing

Referências



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



Exploits que irei mostrar

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências

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

Exemplo

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências

Problemas:

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

Minha solução

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências

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

Exemplo cabeçalho 1

Exemplo cabeçalho 2

Exemplo cabeçalho 3

Exemplo **Negrito**

Exemplo *italico*



Exemplo cabeçalho 1

Exemplo cabeçalho 2

Exemplo cabeçalho 3

Exemplo **Negrito**

Exemplo *italico*

Minha solução

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências

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**

ARP Spoofing

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências

site HTTP não seguro de propósito:

`http://testing-ground.scraping.pro/login`

Softwares de defesa :

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

Outra solução

HTTPS



Mitigação de arp spoofing,
<http://antidote.sourceforge.net/>.



Cve, <https://cve.mitre.org/>.



Estatísticas de vulnerabilidades,
<https://cve.mitre.org/>.



S. Jajodia and C. Mazumdar, *Information systems security: First international conference, iciss 2005, kolkata, india, december 19-21, 2005, proceedings*, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2005.



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_\(XSS\)/](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)/).

Obrigado

Segurança em
redes

Giuliano Oliveira
de Macedo

Importância de
segurança em
redes

Contextualização

Ataques

XSS

ARP Spoofing

Referências

Código fonte dos exploits e desse slide estão disponíveis no repositório github:

<https://github.com/llpinokio/rc2t2>