HaXF4RALL
Hackers Repository

What is CTF and how to get Started – Complete Guide for Beginners to Advanced

June 29, 2019

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Table of Contents - (Click on Section to Jump to)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

What is Capture the Flag - CTF

CTF's (capture the flag) are computer security/hacking competitions which generally consist of participants breaking, investigating, reverse engineering and doing anything they can to reach the end goal, a "flag" which is usually found as a string of text.

DEF CON hosts what is the most widely known and first major CTF, occuring annualy at the hacking conference in Las Vegas. Many different competitions have branched off since then, and numerous ones are available year round. One of the best places to see when CTFs are being scheduled is ctftime, an active website with calendars and team rankings.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Example

A very simple type of CTF challenge consists of looking at the source code of websites or programs to find flags that looks like a string – “35k325j4hnlsdfjxc” or a hint like “user agent: /disallow secret ” (now we know there’s a secret directory, which might have some leads to get the next flag) to complete/obtain the flag.

Why use CTF

Computer security represents a challenge to education due to its interdisciplinary nature. Topics in computer security are drawn from areas ranging from theoretical aspects of computer science to applied aspects of information technology management. This makes it difficult to encapsulate the spirit of what constitutes a computer security professional.

One approximation for this measure has emerged: the ‘capture the flag’ competition. Attack-oriented CTF competitions try to distill the essence of many aspects of professional

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

computer security work into a single short exercise that is objectively measurable. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.

A modern computer security professional should be an expert in at least one of these areas and ideally in all of them. Success in CTF competitions demands that participants be an expert in at least one and ideally all of these areas. Therefore, preparing for and competing in CTF represents a way to efficiently merge discrete disciplines in computer science into a focus on computer security.

What should I focus on?

Difficulty is subjective based on your individual skillset. If your forte is forensics but you are not skilled in crypto, the point values assigned to the forensics problems will seem inflated while the crypto challenges will seem undervalued to you. The same perception biases hold true for CTF organizers. This is one reason why assessing the difficulty of CTF problems is so challenging.

If you've tried several of the basic problems on your own and are still struggling, then there are plenty of self-study opportunities. CTF competitions generally focus on the following skills: reverse engineering, cryptography, ACM style programming, web vulnerabilities, binary exercises, networking, and forensics. Pick one and focus on a single topic as you get started.

1) Reverse Engineering. I highly suggest that you get a copy of IDA Pro. There is a free version available as well as a discounted student license. Try some crack me exercises. Write your own C code and then reverse the compiled versions. Repeat this process while changing

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

compiler options and program logic. How does an “if” statement differ from a “select” in your compiled binary? I suggest you focus on a single architecture initially: x86, x86_64, or ARM. Read the processor manual for whichever one you choose. Book recommendations include:

- Practical Reverse Engineering
- Reversing: Secrets of Reverse Engineering
- The IDA Pro Book

2) Cryptography. Here are some resources to check out:

- Applied Cryptography
- Practical Cryptography
- Cyber Security Career Bundle Course

3) ACM style programming. Pick a high level language. I recommend Python or Ruby. For Python, read Dive into Python (free) and find a pet project you want to participate in. It is worth noting that Metasploit is written in Ruby. Computer science classes dealing with algorithms and data structures will go a long way in this category as well. Look at past programming challenges from CTF and other competitions – do them! Focus on creating a working solution rather than the fastest or most elegant solution, especially if you are just getting started.

4) Web vulnerabilities. There are many web programming technologies out there. The most popular in CTF tend to be PHP and SQL. The php.net site is a fantastic language reference. Just search any function you are curious about. After PHP, the next most common way to see web challenges presented is with Python or Ruby scripts. Notice the overlap of skills?

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

There is a good book on web vulnerabilities, The Web Application Hacker's Handbook. Other than that, after learning some of the basic techniques, you might also think about gaining expertise in a few of the more popular free tools available. These are occasionally useful in CTF competitions too. This category also frequently overlaps with cryptography in my experience.

5) Binary exercises. I recommend you go through reverse engineering before jumping into the binary exercises. There are a few common vulnerability types you can learn in isolation: stack overflows, heap overflows, and format string bugs for starters. A lot of this is training your mind to recognize vulnerable patterns. Looking at past vulnerabilities is a great way to pick up these patterns. You should also read through:

- Hacking: The Art of Exploitation
- The Shellcoders Handbook
- The Art of Software Security Assessment

6) Forensics/networking. A lot of CTF teams tend to have "the" forensics guy. Learn how to use the 010 hex editor and don't be afraid to make absurd, wild, random guesses as to what could be going on in some of these problems.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Finding a CTF

If you ever wanted to start running, you were probably encouraged to sign up to a 5k to keep focused on a goal. The same principle applies here: pick a CTF in the near future that you want to compete in and come up with a practice schedule. Here are some CTFs that we can recommend:

- PicoCTF and PlaidCTF by CMU
- HSCTF is made for high school students
- Ghost in the Shellcode (GitS)
- CSAW CTF by NYU-Poly
- UCSB iCTF is for academics only
- Defcon CTF

Visit CTF Time and the CapCTF calendar for a more complete list of CTFs occuring every week of the year.

How is a Wargame different?

Wargames are similar to a CTF but are always ongoing. Typically, they are organized into levels that get progressively harder as you solve more of them. Wargames are an excellent way to practice for CTF! Here are some of our favorites:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Micro Corruption
- SmashTheStack
- OverTheWire
- Exploit Exercises

What about CCDC?

There are some defense-only competitions that disguise themselves as CTF competitions, mainly the Collegiate Cyber Defense Challenge (CCDC) and its regional variations, and our opinion is that you should avoid them. They are unrealistic exercises in frustration and will teach you little about security or anything else. They are incredibly fun to play as a Red Team though!

Using the Field and Resources Guide

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

> “Knowing is not enough; we must apply. Willing is not enough; we must do.” – Johann Wolfgang von Goethe

CTF Field Guide – Field Guide by Trails of Bits

If you’re going to make a living in defense, you have to think like the offense.

So, learn to win at Capture The Flag (CTF). These competitions distill major disciplines of professional computer security work into short, objectively measurable exercises. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.

Whether you want to succeed at CTF, or as a computer security professional, you’ll need to become an expert in at least one of these disciplines. Ideally in all of them.

That’s why we (Trails of Bits) wrote this book.

In these chapters, you’ll find everything you need to win your next CTF competition:

- Walkthroughs and details on past CTF challenges
- Guidance to help you design and create your own toolkits
- Case studies of attacker behavior, both in the real world and in past CTF competitions

To make your lives easier, we’ve supplemented each lesson with the Internet’s best supporting reference materials. These come from some of the best minds in the computer

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

security field. Looking ahead, we hope you'll collaborate to keep this book evolving with the industry.

We've tried to structure this so you can learn as quickly as you want, but if you have questions along the way, contact us. We'll direct your question to the most relevant expert. If there's enough demand, we may even schedule an online lecture.

CTF Resources - Start Guide maintained by community

These docs are organized broadly along the lines by which CTF tasks are organized. Inside each folder in the topics section is a README like this one explaining the basics of the technology and what the tasks generally involve. Alongside these READMES are folders with more information regarding specific technologies and topics. Many of these articles link to the tools folder, where more detailed explanations can be found for tehcnologies used throughout CTF competitions.

The best way to use these docs is to participate in an actual CTF! Join a CTF or attempt some old tasks and try to solve them. Use the information in this repository to get you started with finding some flags. If you feel like there is insufficient information to help you solve a task, bring up an issue on this repository and someone can try to clarify it.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tools Used for Solving CTF

Tools used for solving CTF challenges

Attacks

Tools used for performing various kinds of attacks

- Bettercap – Framework to perform MITM (Man in the Middle) attacks.
- Layer 2 attacks – Attack various protocols on layer 2

Crypto

Tools used for solving Crypto challenges

- FeatherDuster – An automated, modular cryptanalysis tool
- Hash Extender – A utility tool for performing hash length extension attacks
- PkCrack – A tool for Breaking PkZip-encryption
- RSACTFTool – A tool for recovering RSA private key with various attack

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- RSATool – Generate private key with knowledge of p and q
- XORTool – A tool to analyze multi-byte xor cipher

Bruteforcers

Tools used for various kind of bruteforcing (passwords etc.)

- Hashcat – Password Cracker
- John The Jumbo – Community enhanced version of John the Ripper
- John The Ripper – Password Cracker
- Nozzlr – Nozzlr is a bruteforce framework, trully modular and script-friendly.
- Ophcrack – Windows password cracker based on rainbow tables.
- Patator – Patator is a multi-purpose brute-forcer, with a modular design.

Exploits

Tools used for solving Exploits challenges

- DLLInjector – Inject dlls in processes
- libformatstr – Simplify format string exploitation.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Metasploit – Penetration testing software
- one_gadget – A tool to find the one gadget
- Pwntools – CTF Framework for writing exploits
- Qira – QEMU Interactive Runtime Analyser
- ROP Gadget – Framework for ROP exploitation
- V0lt – Security CTF Toolkit

Forensics

Tools used for solving Forensics challenges

- Aircrack-Ng – Crack 802.11 WEP and WPA-PSK keys
  - `apt-get install aircrack-ng`
- Audacity – Analyze sound files (mp3, m4a, whatever)
  - `apt-get install audacity`
- Bkhive and Samdump2 – Dump SYSTEM and SAM files
  - `apt-get install samdump2 bkhive`
- CFF Explorer – PE Editor

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Creddump – Dump windows credentials
- DVCS Ripper – Rips web accessible (distributed) version control systems
- Exif Tool – Read, write and edit file metadata
- Extundelete – Used for recovering lost data from mountable images
- Fibratus – Tool for exploration and tracing of the Windows kernel
- Foremost – Extract particular kind of files using headers
    - `apt-get install foremost`
- Fsck.ext4 – Used to fix corrupt filesystems
- Malzilla – Malware hunting tool
- NetworkMiner – Network Forensic Analysis Tool
- PDF Streams Inflater – Find and extract zlib files compressed in PDF files
- ResourcesExtract – Extract various filetypes from exes
- Shellbags – Investigate NT_USER.dat files
- UsbForensics – Contains many tools for usb forensics
- Volatility – To investigate memory dumps

Registry Viewers

- RegistryViewer – Used to view windows registries
- Windows Registry Viewers – More registry viewers

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Networking

Tools used for solving Networking challenges

- Bro – An open-source network security monitor.
- Masscan – Mass IP port scanner, TCP port scanner.
- Monit – A linux tool to check a host on the network (and other non-network activities).
- Nipe – Nipe is a script to make Tor Network your default gateway.
- Nmap – An open source utility for network discovery and security auditing.
- Wireshark – Analyze the network dumps.
    - `apt-get install wireshark`
- Zmap – An open-source network scanner.

Reversing

Tools used for solving Reversing challenges

- Androguard – Reverse engineer Android applications
- Angr – platform-agnostic binary analysis framework
- Apk2Gold – Yet another Android decompiler

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- ApkTool – Android Decompiler
- Barf – Binary Analysis and Reverse engineering Framework
- Binary Ninja – Binary analysis framework
- BinUtils – Collection of binary tools
- BinWalk – Analyze, reverse engineer, and extract firmware images.
- Boomerang – Decompile x86 binaries to C
- ctf_import – run basic functions from stripped binaries cross platform
- Frida – Dynamic Code Injection
- GDB – The GNU project debugger
- GEF – GDB plugin
- Ghidra – Open Source suite of reverse engineering tools. Similar to IDA Pro.
- Hopper – Reverse engineering tool (disassembler) for OSX and Linux
- IDA Pro – Most used Reversing software
- Jadx – Decompile Android files
- Java Decompilers – An online decompiler for Java and Android APKs
- Krakatau – Java decompiler and disassembler
- Objection – Runtime Mobile Exploration
- PEDA – GDB plugin (only python2.7)
- Pin A dynamic binary instrumentaion tool by Intel
- Plasma – An interactive disassembler for x86/ARM/MIPS which can generate indented pseudo-code with colored syntax.
- Pwndbg – A GDB plugin that provides a suite of utilities to hack around GDB easily.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- radare2 – A portable reversing framework
- Triton – Dynamic Binary Analysis (DBA) framework
- Uncompyle – Decompile Python 2.7 binaries (.pyc)
- WinDbg – Windows debugger distributed by Microsoft
- Xocopy – Program that can copy executables with execute, but no read permission
- Z3 – a theorem prover from Microsoft Research

JavaScript Deobfuscators

- Detox – A Javascript malware analysis tool
- Revelo – Analyze obfuscated Javascript code

SWF Analyzers

- RABCDAsm – Collection of utilities including an ActionScript 3 assembler/disassembler.
- Swftools – Collection of utilities to work with SWF files
- Xxxswf – A Python script for analyzing Flash files.

Services

Various kind of useful services available around the internet

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- CSWSH – Cross-Site WebSocket Hijacking Tester
- Request Bin – Lets you inspect http requests to a particular url

Steganography

Tools used for solving Steganography challenges

- Convert – Convert images b/w formats and apply filters
- Exif – Shows EXIF information in JPEG files
- Exiftool – Read and write meta information in files
- Exiv2 – Image metadata manipulation tool
- ImageMagick – Tool for manipulating images
- Outguess – Universal steganographic tool
- Pngtools – For various analysis related to PNGs
    - `apt-get install pngtools`
- SmartDeblur – Used to deblur and fix defocused images
- Steganabara – Tool for stegano analysis written in Java
- Stegbreak – Launches brute-force dictionary attacks on JPG image
- StegCracker – Steganography brute-force utility to uncover hidden data inside files
- stegextract – Detect hidden files and text in images

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Steghide – Hide data in various kind of images
- Stegsolve – Apply various steganography techniques to images
- Zsteg – PNG/BMP analysis

Web

Tools used for solving Web challenges

- BurpSuite – A graphical tool to testing website security.
- Commix – Automated All-in-One OS Command Injection and Exploitation Tool.
- Hackbar – Firefox addon for easy web exploitation
- OWASP ZAP – Intercepting proxy to replay, debug, and fuzz HTTP requests and responses
- Postman – Add on for chrome for debugging network requests
- Raccoon – A high performance offensive security tool for reconnaissance and vulnerability scanning
- SQLMap – Automatic SQL injection and database takeover tooli
- W3af – Web Application Attack and Audit Framework.
- XSSer – Automated XSS testor

Latest Tools Released

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Visit our Tools directory or home page on all the latest tools released in the hacking community.

Sites with daily updated hacking tools

- Haxf4rall
- Sectechno
- Cyberpunk
- Darknet
- Securityonline
- Blackhat
- Kitploit
- HackwithGithub – Awesome Hacking
- Prodefence
- HackersOnlineClub

Starter Packs

Collections of installer scripts, useful tools

- CTF Tools – Collection of setup scripts to install various security research tools.
- LazyKali – A 2016 refresh of LazyKali which simplifies install of tools and configuration.
- Seclists – Pentesters Companion

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- PayloadAllTheThings – A list of useful payloads and bypass for Web Application Security and Pentest/CTF
- Awesome-Pentest – A collection of awesome penetration testing resources supported by netsparker
- Exploit Pack – The offensive side of the Fence

Operating Systems

Penetration testing and security lab Operating Systems

- Android Tamer – Based on Debian
- BackBox – Based on Ubuntu
- BlackArch Linux – Based on Arch Linux
- Fedora Security Lab – Based on Fedora
- Kali Linux – Based on Debian
- Parrot Security OS – Based on Debian
- Pentoo – Based on Gentoo
- URIX OS – Based on openSUSE
- Wifislax – Based on Slackware

Malware analysts and reverse-engineering

- Flare VM – Based on Windows

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- REMnux – Based on Debian

Wikis

Various Wikis available for learning about CTFs

- Bamboofox – Chinese resources to learn CTF
- ISIS Lab – CTF Wiki by Isis lab
- OpenToAll – Open To All Knowledge Base

Online CTF Platforms & Wargames

Always online CTFs

- Backdoor – Security Platform by SDSLabs.
- Crackmes – Reverse Engineering Challenges
- Ctfs.me – CTF All the time
- Exploit Exercises – Variety of VMs to learn variety of computer security issues.
- Gracker – Binary challenges having a slow learning curve, and write-ups for each level.

- Hack The Box – Weekly CTFs for all types of security enthusiasts.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Hack This Site – Training ground for hackers.
- Hacking-Lab – Ethical hacking, computer network and security challenge platform.
- Hone Your Ninja Skills – Web challenges starting from basic ones.
- IO – Wargame for binary challenges.
- Microcorruption – Embedded security CTF
- Over The Wire – Wargame maintained by OvertheWire Community
- Pwnable.kr – Pwn Game
- Pwnable.tw – Binary wargame
- Pwnable.xyz – Binary Exploitation Wargame
- Reversin.kr – Reversing challenge
- Ringzer0Team – Ringzer0 Team Online CTF
- Root-Me – Hacking and Information Security learning platform.
- ROP Wargames – ROP Wargames
- SmashTheStack – A variety of wargames maintained by the SmashTheStack Community.
- VulnHub – VM-based for practical in digital security, computer application & network administration.
- W3Challs – A penetration testing training platform, which offers various computer challenges, in various categories.
- WebHacking – Hacking challenges for web.
- WeChall – Always online challenge site.

- WTHack OnlineCTF – CTF Practice platform for every level of cyber security

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

enthusiasts.

CTF Writeups

Collections of CTF write-ups

- Captf – Dumped CTF challenges and materials by psifertex
- CTF write-ups (community) – CTF challenges + write-ups archive maintained by the community
- CTFTime Scrapper – Scraps all writeup from ctf time and organize which to read first
- pwntools writeups – A collection of CTF write-ups all using pwntools
- Shell Storm – CTF challenge archive maintained by Jonathan Salwan
- Smoke Leet Everyday – CTF write-ups repo maintained by SmokeLeetEveryday team.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Creating your own CTF machine

Tools used for creating CTF challenges

Forensics

Tools used for creating Forensics challenges

- Dnscat – Hosts communication through DNS
- Registry Dumper – Dump your registry

Platforms

Projects that can be used to host a CTF

- CTFd – Platform to host jeopardy style CTFs from ISISLab, NYU Tandon
- FBCTF – Platform to host Capture the Flag competitions from Facebook
- HackTheArch – CTF scoring platform
- Mellivora – A CTF engine written in PHP

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- NightShade – A simple security CTF framework
- OpenCTF – CTF in a box. Minimal setup required
- PicoCTF Platform 2 – A genericized version of picoCTF 2014 that can be easily adapted to host CTF or programming competitions.
- PyChallFactory – Small framework to create/manage/package jeopardy CTF challenges
- RootTheBox – A Game of Hackers (CTF Scoreboard & Game Manager)
- Scorebot – Platform for CTFs by Legitbs (Defcon)
- SecGen – Security Scenario Generator. Creates randomly vulnerable virtual machines

Steganography

Tools used to create stego challenges

- Convert – Convert images b/w formats and apply filters
- Exif – Shows EXIF information in JPEG files
- Exiftool – Read and write meta information in files
- Exiv2 – Image metadata manipulation tool
- ImageMagick – Tool for manipulating images
- Outguess – Universal steganographic tool

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Pngtools – For various analysis related to PNGs
    - `apt-get install pngtools`
- SmartDeblur – Used to deblur and fix defocused images
- Steganabara – Tool for stegano analysis written in Java
- Stegbreak – Launches brute-force dictionary attacks on JPG image
- StegCracker – Steganography brute-force utility to uncover hidden data inside files
- stegextract – Detect hidden files and text in images
- Steghide – Hide data in various kind of images
- Stegsolve – Apply various steganography techniques to images
- Zsteg – PNG/BMP analysis

Web

Tools used for creating Web challenges

JavaScript Obfustcators

- Metasploit JavaScript Obfuscator
- Uglify

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

References

Used references in this article

- http://captf.com/
- https://trailofbits.github.io
- https://ctfs.github.io
- https://www.endgame.com/blog/technical-blog/how-get-started-ctf
- https://github.com/apsdehal/awesome-ctf
- https://github.com/toolswatch/blackhat-arsenal-tools
- All CTF platforms/wargames and tool websites listed on this page.

Credits to all the creators listed above for their awesome work

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

« InfectionMonkey – Breach and Attack Simulation Tool to Evaluate the Security of your Network

HAL – The Hardware Analyzer »

Related Articles

Translate

Select Language ▼

Powered by Google Translate

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

DSTIKE WIFI DEAUTHER OLED

~~$19.00~~ $16.00

ADD TO CART

CACTUS WHID: WIFI HID INJECTOR USB RUBBER DUCKY/KEYLOGGER

$25.00

ADD TO CART

WIRELESS ZIGBEE CC2531 SNIFFER BARE BOARD USB PACKET ANALYZER

~~$6.00~~ $5.00

ADD TO CART

THROWING STAR LAN TAP

$12.00 – $16.00

SELECT OPTIONS

BLUEFRUIT BLE FRIEND NRF51822 V3.0 DEVELOPMENT BOARD

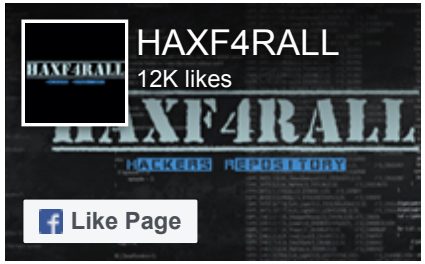
$38.00

ADD TO CART

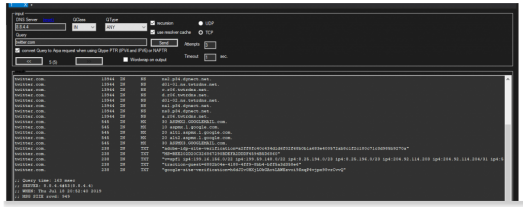
Follow Us

Create PDF in your applications with the Pdfcrowd HTML to PDF API

PDFCROWD



Recent Posts



Cazador – WebApp Pentest Toolkit

October 9, 2019

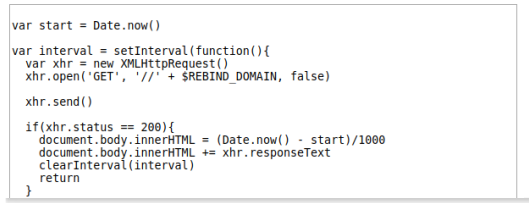
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Sub.Sh – Online Subdomain Detect Script

October 8, 2019

PatrOwl – Smart and Scalable Security Operations Orchestration Platform

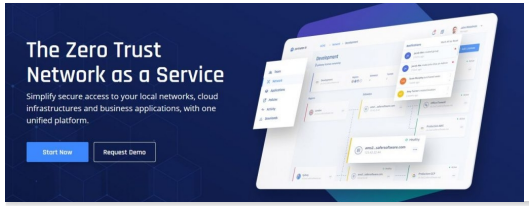
October 7, 2019



```
var start = Date.now()

var interval = setInterval(function(){
  var xhr = new XMLHttpRequest()
  xhr.open('GET', '//' + $REBIND_DOMAIN, false)

  xhr.send()

  if(xhr.status == 200){
    document.body.innerHTML = (Date.now() - start)/1000
    document.body.innerHTML += xhr.responseText
    clearInterval(interval)
    return
  }
```

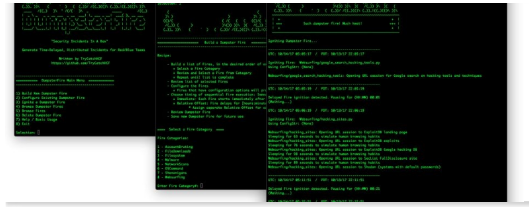
DNS Rebinding Tool – DNS Rebind Tool With Custom Scripts

October 6, 2019



Perimeter 81 – The Zero Trust Network as a Service

October 5, 2019



DumpsterFire Toolset – Security Incidents In A Box!

October 4, 2019

Create PDF in your applications with the Pdfcrowd HTML to PDF API
PDFCROWD

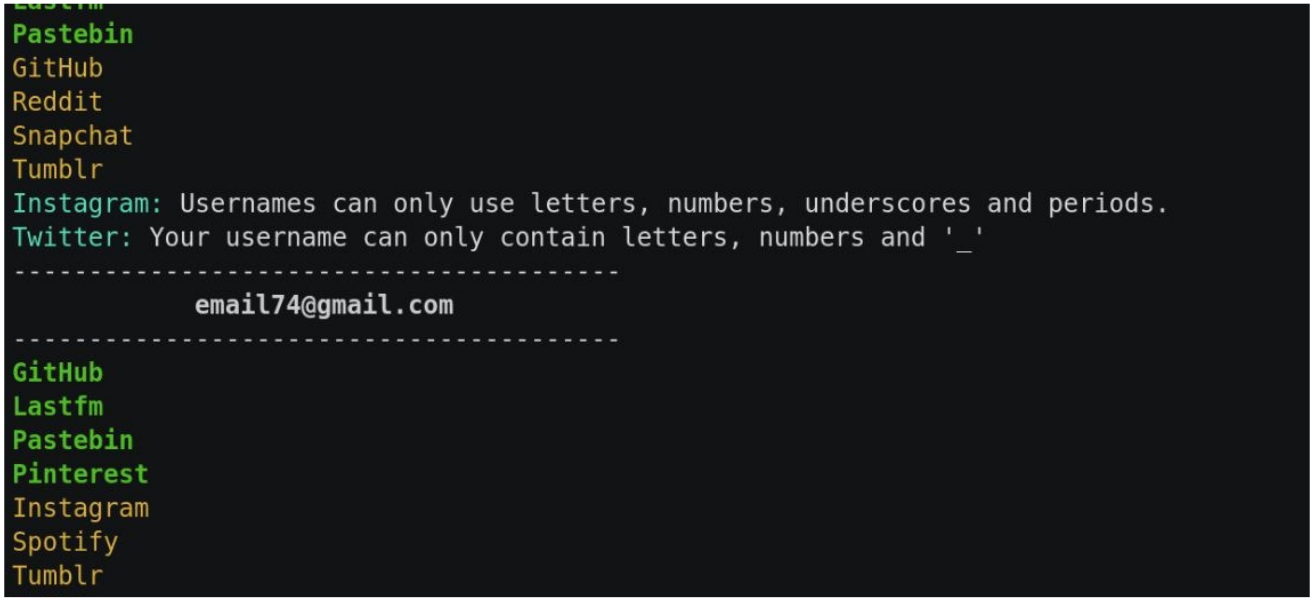
HACKER STICKERS 50PCS

Popular Posts

- Huge Collection of Deep Web Onion Links
- 100 working deep web, onion and dark web links
- xPlay and Onion Porn Sites
- IP Booter for PS4 and Xbox
- PatrOwl - Smart and Scalable Security Operations Orchestration Platform
- How to kick players Offline on PS4 / Xbox One
- Sub.Sh - Online Subdomain Detect Script

Social Media Hacking

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

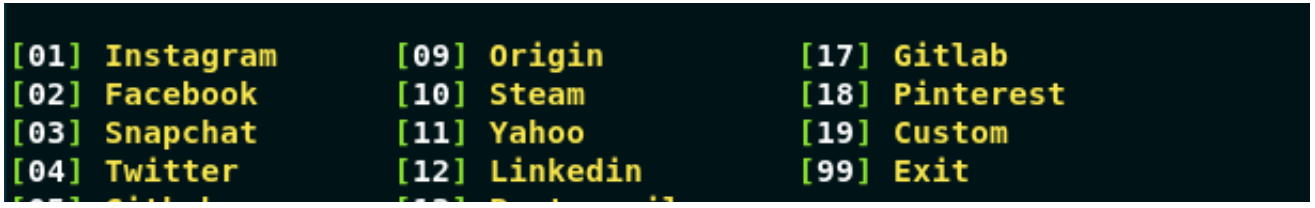


SocialScan – Check Email Address and Username Availability on Online Platforms

- Social Media Hacking

June 17, 2019

Give an email address or username, socialscan returns whether it is available, taken or invalid on online platforms. Its speed...



Shellphish – Phishing Tool For 18 Social Media Apps

June 10, 2019

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

WhatsApp Hacking using QRLJacking

May 2, 2019

How to Hack any Facebook Account with Z-Shadow

April 26, 2019

TeleKiller – A Tools Session Hijacking And Stealer Local Passcode Telegram Windows

April 15, 2019

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

3D SKULL BUFFS – FACE MASKS

ABOUT US

Haxf4rall is a collective, a good starting point and provides a variety of quality material for cyber security professionals.

COMPANY

RESOURCES

TOOLBOX

Create PDF in your applications with the Pdfcrowd HTML to PDF API

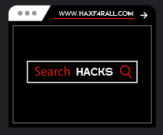
PDFCROWD

Our primary focus revolves around the latest tools released in the Infosec community and provide a platform for developers to showcase their skillset and current projects.

Live Chat

Get Started

Tools Directory



HACKERS REPOSITORY

2014 – 2019 | Haxf4rall.com

Stay Connected:

Create PDF in your applications with the Pdfcrowd HTML to PDF API

PDFCROWD