

The background is a dark gray to black gradient. It features several concentric circles and arcs of varying sizes. Some of these arcs have small tick marks and numerical degree values (e.g., 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) along their circumference. There are also small arrows pointing in different directions, suggesting a sense of rotation or movement. The overall aesthetic is technical and geometric.

CATEGORY WEB

FANTASTIC TALES OF CAPTURE-THE-FLAG (CTF) CHALLENGES PAST

OWASP TORONTO – MAY 25, 2017

whoami

- Jamie Baxter (@jmbxtr)
- Independent Information Security Consultant focusing on security assessments [SRNSEC]
- Previously worked in aerospace, government and finance sectors
- CTF'er, pen-tester, appsec, certs [OSCP, OSCE, CISSP, GPEN]
- Course Developer & Instructor for York School of Continuing Studies - Cyber Security Program.
- Team Lead for Bsidess Ottawa CTF last 3 years
- Team Captain of "SomeRandomName"



WHAT'S A CTF

A CTF or Capture the Flag is a computer security competition.

- Jeopardy (Like Ottawa Bsides CTF)
- Attack and Defense
- Quest

The problems will often cross wide range of computer security subject areas such as:

Application Security (IE. Web), Trivia, cryptography, forensics (image, file, memory), binary analysis, reverse engineering, exploit development, mobile security and moar!

Level of a difficulty and focus will vary from event to event. Ex

- EasyCTF/ PicoCTF – Introductory – Great Place to Start
- CSAW / Bsides Ottawa wide range of problems
- Defcon – Heavy Binary Analysis/Exploitation focus

WHAT'S A WARGAME

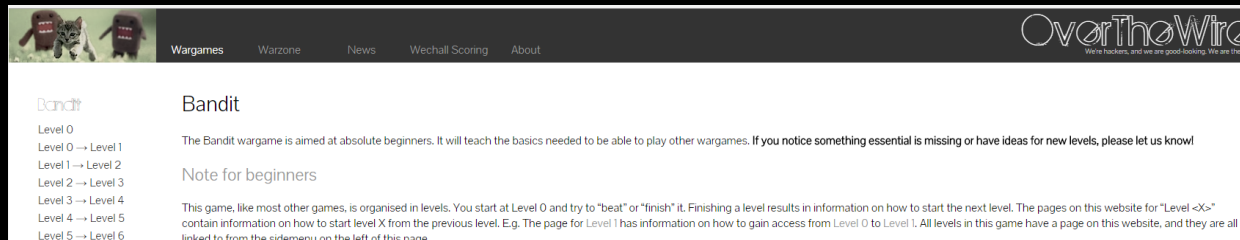
A series of primarily individual challenges always available to practice security skills

Typically available 24/7/365

- Over the Wire - <http://overthewire.org> -> BANDIT
- Smash The Stack - <http://smashtthestack.org/>
- Microcorruption - <https://microcorruption.com/>
- Ringer Zero - <https://ringzer0team.com/> (also a collection of many past ctf problems)

Multiple levels, going from easier to harder.

START HERE



CTFING THEN AND NOW

- First CTF – Defcon 4 - 1996
- Hundreds of onsite and online events in 2017
- There's a major online CTF almost every weekend
- Global rankings at **ctftime.org**

NSEC
Applied Security Competition in North
America

CTF TIME

CTFsUpcomingArchiveCalendarTeamsFAQContact usAbout

Team rating

2017201620152014201320122011

Place	Team	Country	Rating
1	dcua	🇺🇦	213.886
2	p4	🇷🇺	149.774
3	Dragon Sector	🇷🇺	137.999
4	HITCON	🇹🇼	130.139
5	BostonKeyParty	🇺🇸	120.000
6	CodiSec	🇷🇺	117.802
7	Tasteless		102.619
8	Plaid Parliament of Pwning	🇺🇸	101.730
9	OpenToAll		91.343
10	b1oOp		

coming e

anHigh-Scho

natName

VolgaCTFOn-line

Insomni'haxSwitzer

angstromOn-line

Now running

OCTF 2017 Quals

266 teams

On-line

Sat, March 18, 2017 00:00 — Mon, March 20, 00:00 UTC

(19m more)

Past events

With scoreboardAll

Pragyan CTF 2017

March 05, 2017 18:30 UTC | On-line

Place	Team	Country	Points
1	dcua	🇺🇦	0.000
2	khack40	🇫🇷	0.000
3	parth		0.000

A APPROACH FOR CTF WEB PROBLEMS

Reconnaissance

- Service Scan
- Spider (Manual or Automated)
- Directory And File Enumeration
- Common Files
 - robots.txt, .git repos, editing artifacts (.index.php, index.php~)
- Enumerate Features (login page, file upload page, file browsing, database)
- Anything Weird?
 - Odd Server Headers
 - Comments in Source Code
 - Parameters



Mapping

- Identify sources of users controllable input
 - Headers
 - Cookie Parameters
 - Hashes
 - Base64 Encoded
 - File Uploads
 - Forms
 - Parameters (POST / GET)
- Identify Any Crypto Use
- Use of Databases
- XSS Related Challenge
- Other functionality (Templates, XML Processing, Deserialization)



Analysis

- Dynamic Analysis
 - Fuzzing
 - Polygots
 - Payload Lists
 - Bit Flipper
 - Brute Forcers
 - XXE Testing
 - Template Testing
 - Deserialization Testing
- Static Analysis
 - Code Review
 - Research



Exploitation

- Payload Construction
- Evasions
- Find the Flag!

TOOLS OF THE TRADE

- Proxy (Burp, Zap)
- A Good Database of Test Strings (SecLists, Fuzzdb)
- Dirb
- FeatherDuster
- XOR-Tool
- Custom Python Scripts
- Sqlmap
- Speciality Tools as needed (XXE, SAML Testing, Deserialization Payloads)
- Other Browser Plugins (ProxySwitch, Cookie Editor)

A BASIC 101 CHALLENGE – EASYAUTH

A CHALLENGE FROM BSIDESSF 2017

Please log in!

Username:

Password:

Log in!

Note: bruteforcing is NOT required or allowed here, and could result in a ban! Hint: try guest/guest

*Challenge from Bsidessf 2017

WARMING UP (EASYAUTH)

Login successful!

Setting cookie: auth=username=guest&date=2017-02-13T10:55:01+0000&

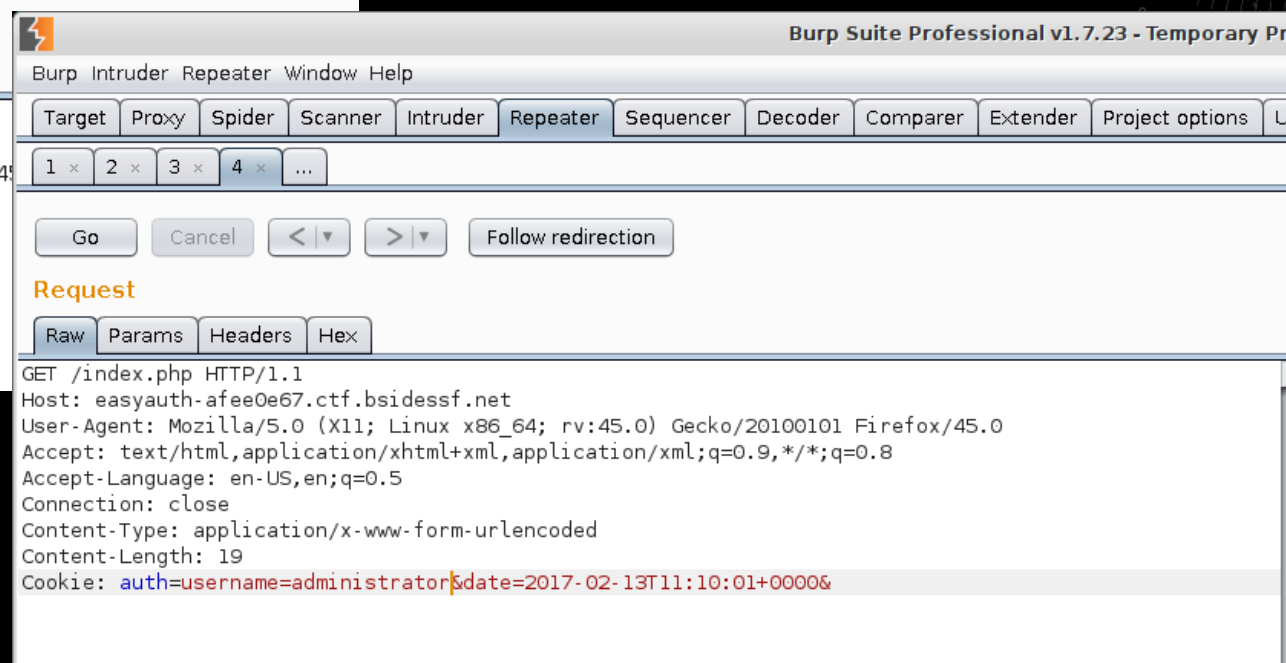
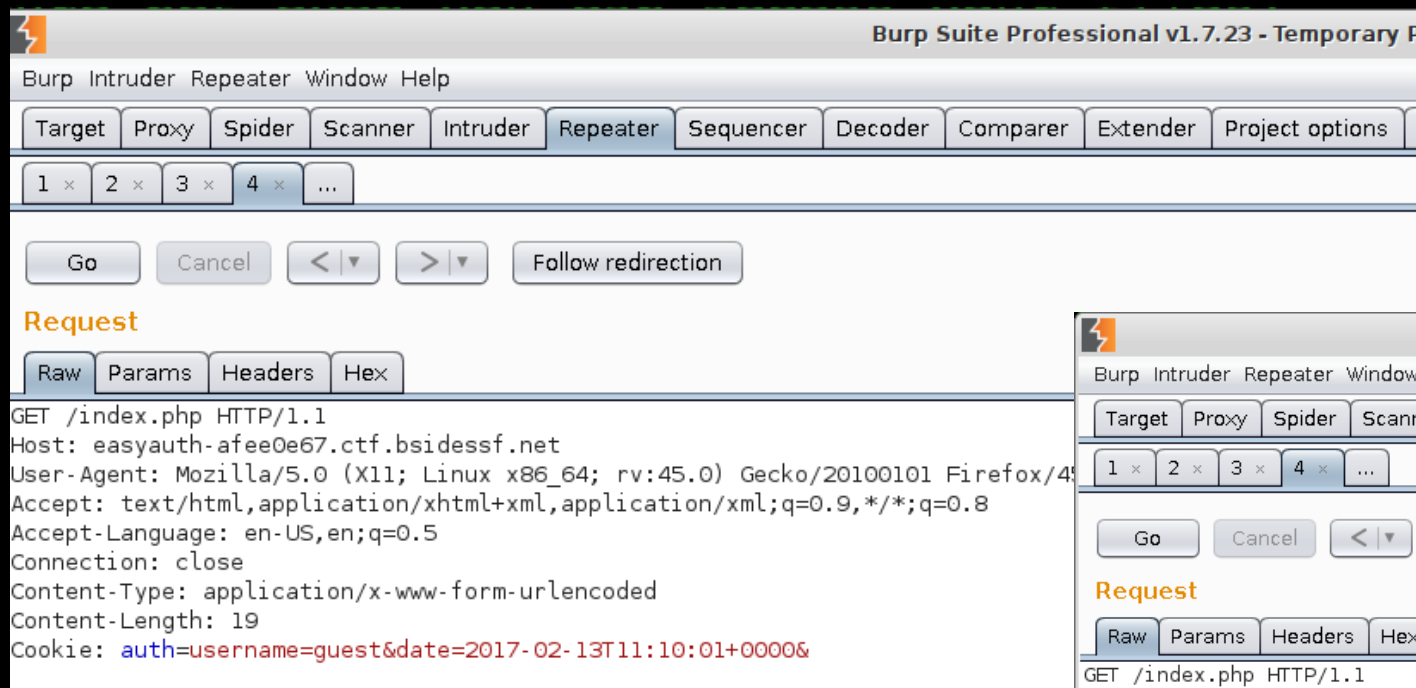
Click [here](#) to continue!

Welcome back, guest!

It's cool that you logged in, but unfortunately we can only give the flag to 'administrator'. :(

[Log out](#)

WARMING UP (EASYAUTH)



A BASIC 101 CHALLENGE

Welcome back, administrator!

Congratulations, you're the administrator! Here's your reward:

FLAG:0076ecde2daae415d7e5ccc7db909e7e

[Log out](#)

More Writeups

<https://github.com/ctfs/write-ups-2017/tree/master/bsidessf-ctf-2017/web/easyauth-30>

```
$cookie = $_COOKIE['auth'];
```

```
$pairs = explode('&', $cookie);
```

```
$args = array();
```

```
foreach($pairs as $pair) {
```

```
    if(!strpos($pair, '='))
```

```
        continue;
```

```
    list($name, $value) = explode('=', $pair, 2);
```

```
    $args[$name] = $value;
```

```
}
```

```
$username = $args['username'];
```

```
print "<h1>Welcome back, $username!</h1>\n";
```

```
if($username == 'administrator') {
```

```
    print "<p>Congratulations, you're the administrator! Here's your  
reward:</p>\n";
```

```
    print "<p>" . FLAG . "</p>\n";
```

```
} else {
```

```
    print "<p>It's cool that you logged in, but unfortunately we can only  
give the flag to 'administrator'. :(</p>\n";
```

```
}
```

WEB200 – COMMAND INJECTION WITH FILTER



BSides Network Monitor

This state of the art network monitor allows you to quickly check if a challenge server is up or down! Enter an IP below in order to check.

This challenge is up! The IP address 127.0.0.1 is alive.

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.019 ms
```

```
--- 127.0.0.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 999ms  
rtt min/avg/max/mdev = 0.018/0.018/0.019/0.004 ms
```

- Simple application to ping
- Two blacklist filters
- Several solutions possible

WEB200 – COMMAND INJECTION WITH FILTER

127.0.0.1; ls Submit

MALICIOUS INPUT DETECTED! PLAY NICE.

- Two filters:
 - Inbound commands filtered for the words/characters in \$badwords
 - Outbound results filtered for the word 'FLAG' – OH NOES DLP!

127.0.0.1 Submit

This challenge is up! The IP address 127.0.0.1 | echo 63617420666c61672e747874 | xxd -r -p | sh is alive.

Detected sensitive info in results - Command Terminated. You were told to play nice...

```
$badwords = array('cd','ls','cat','exec',';','&','more','file','head','less','od','tail','$','xargs','print','=','awk','grep','|','strings','binwalk');
```

WEB200 – COMMAND INJECTION WITH FILTER

127.0.0.1; ls Submit

MALICIOUS INPUT DETECTED! PLAY NICE.

- Two filters:
 - Inbound commands filtered for the words/characters in \$badwords
 - Outbound results filtered for the word 'FLAG' – OH NOES DLP!

127.0.0.1 Submit

This challenge is up! The IP address 127.0.0.1 | echo 63617420666c61672e747874 | xxd -r -p | sh is alive.

Detected sensitive info in results - Command Terminated. You were told to play nice...

```
$badwords = array('cd','ls','cat','exec',';','&','more','file','head','less','od','tail','$','xargs','print','=','awk','grep','|','strings','binwalk');
```

WEB200 – COMMAND INJECTION WITH FILTER

- Intended Solution:
- The initial proof of concept for this challenge involved using a hexdump of the 'cat flag.txt' command and sending the decoded result to sh
- We saw different solutions than this

127.0.0.1

Submit

This challenge is up! The IP address 127.0.0.1 `127.0.0.1 | echo 63617420666c61672e747874 | xxd -r -p | sh | base64` is alive.

RkxBRyA9IHsgQmlsbGllEpvZSBzYXlzlG5pY2UgZ3V5cyBmaW5pc2ggbGFzdC4uLiA6KSB9Cg==

CHALLENGE #1 - REMEMBER ME?

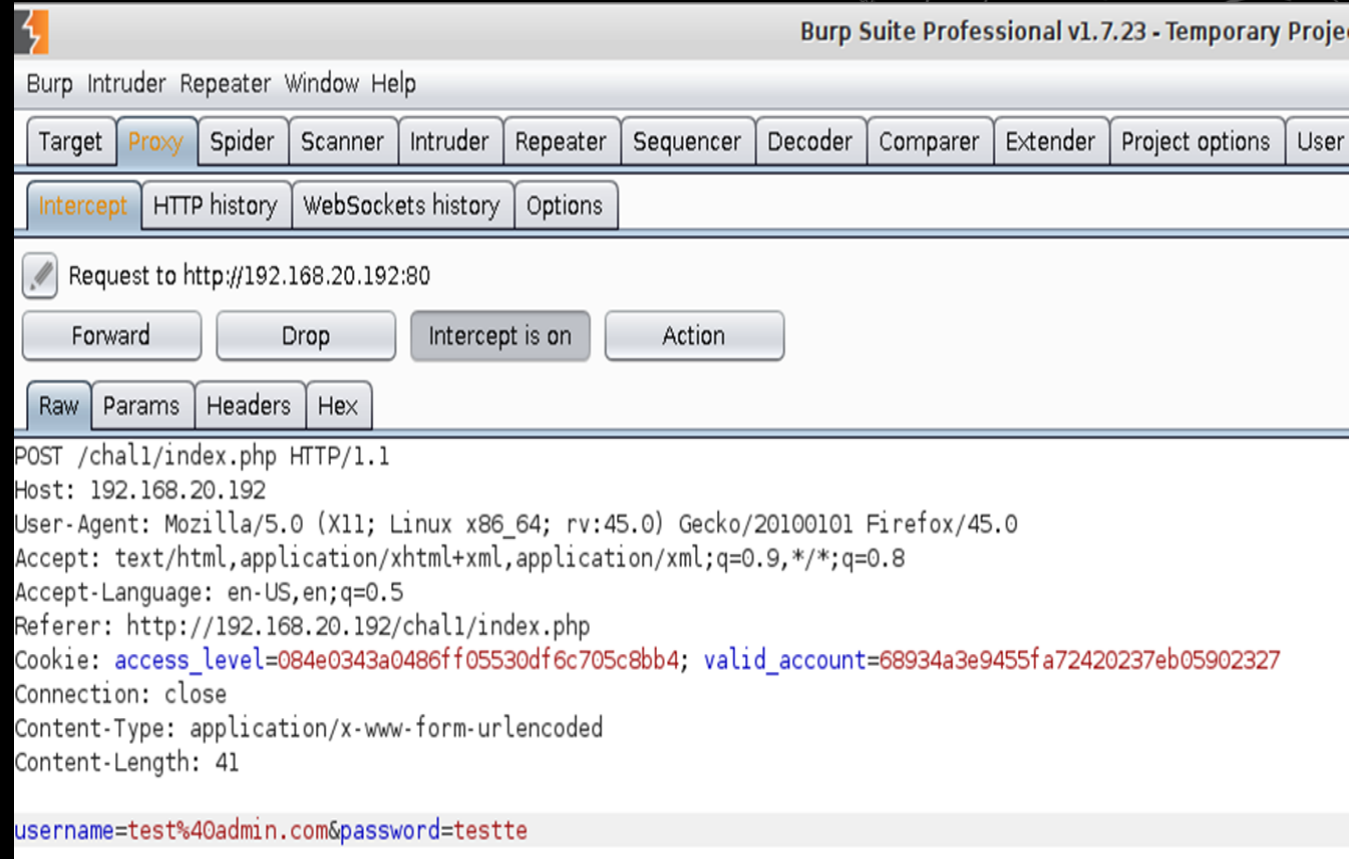
Login in as Admin to
Get Your Flag

☐ Remember me

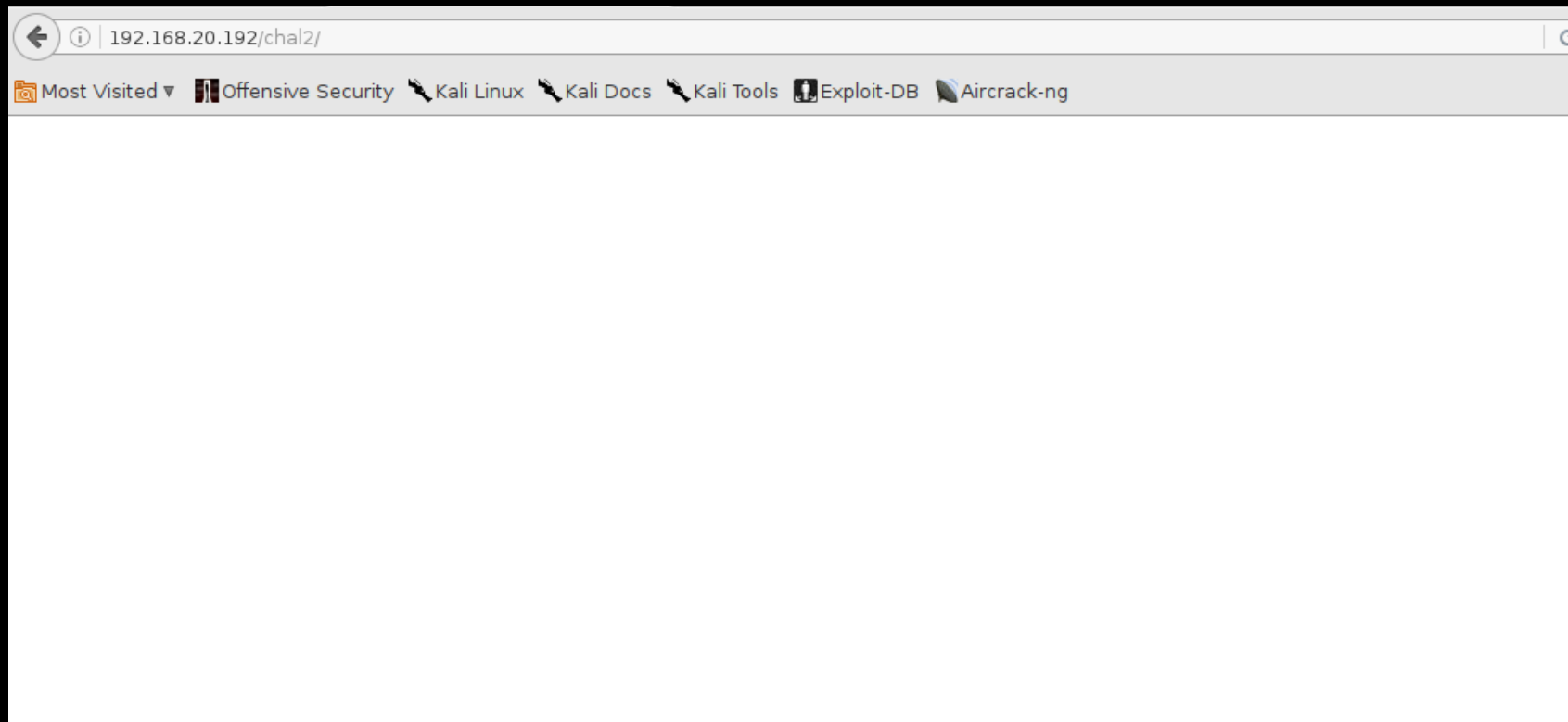
Sign in

Intended Solution

- Google access_level and valid_account hashes to determine it is for guest / false
- Generate hashes for admin and true
- Perform session fixation to elevate privileges
- Get Flag!



CHALLENGE #2 – CATCH ME IF YOU CAN



CHALLENGE #2 – CATCH ME IF YOU CAN

Intended Solution

- Examine page source to find comment referring to admin.php
- Attempt to access admin.php and get redirected.
- Prevent redirection and scroll down admin.php to find command injection
- Locate flag and read
- (Inspired by NSEC 2017 Challenge – Botnet Controller)

CHALLENGE #3 – CYBER FILE VAULT

A vault so secure not even you can access your files!

HALP – I broke the link to my flag, please help me get it back

- [MyPreciousFlag.txt](#)
- [GuideToBeingACyberThoughtLeaderIn30DaysOrLess.txt](#)
- [AutomatedCyberToolsAndU.txt](#)
- [GameOfCybers.txt](#)



CHALLENGE #4 – HACKERNAME GENERATOR

h4ck3r Name Generator

Partial Name:

Submit



Hint

<http://phrack.org/issues/69/12.html>

HOW DO I GET STARTED

- “Solo” CTFs (especially ones like PicoCTF & EasyCTF)
- Review Past – Writeups (<https://github.com/ctfs>)
- Reddit /r/OpenToAllCTFteam has a ongoing team
- Play Online
 - Vulnhub.com
 - ringzer0team.com
 - Smashthestack.org
 - overthewire.org (Start with BANDIT)
- Look out for one off challenges
- If you’re at a SANS event be sure to participate in netwars

WHAT'S COMING UP

- Google CTF June 16
- SECUINSIDE CTF Quals 2017 July 1
- CSAW CTF September
- Any Many Others

