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 Bsides 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

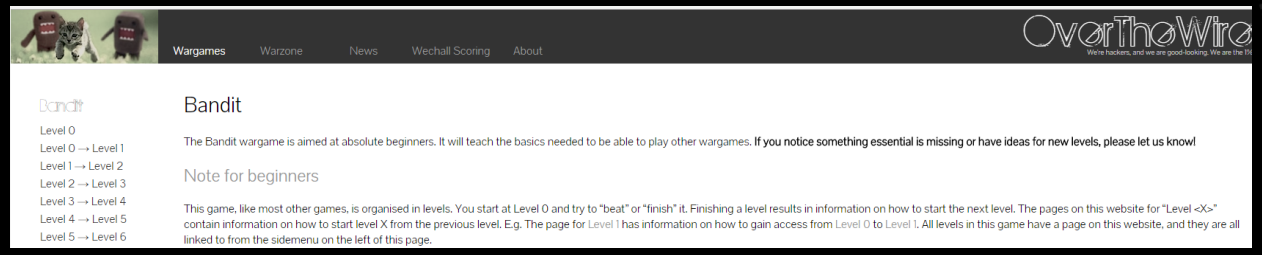
A series of primarily individual challenges always available to practice security skills

Typically available 24/7/365

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

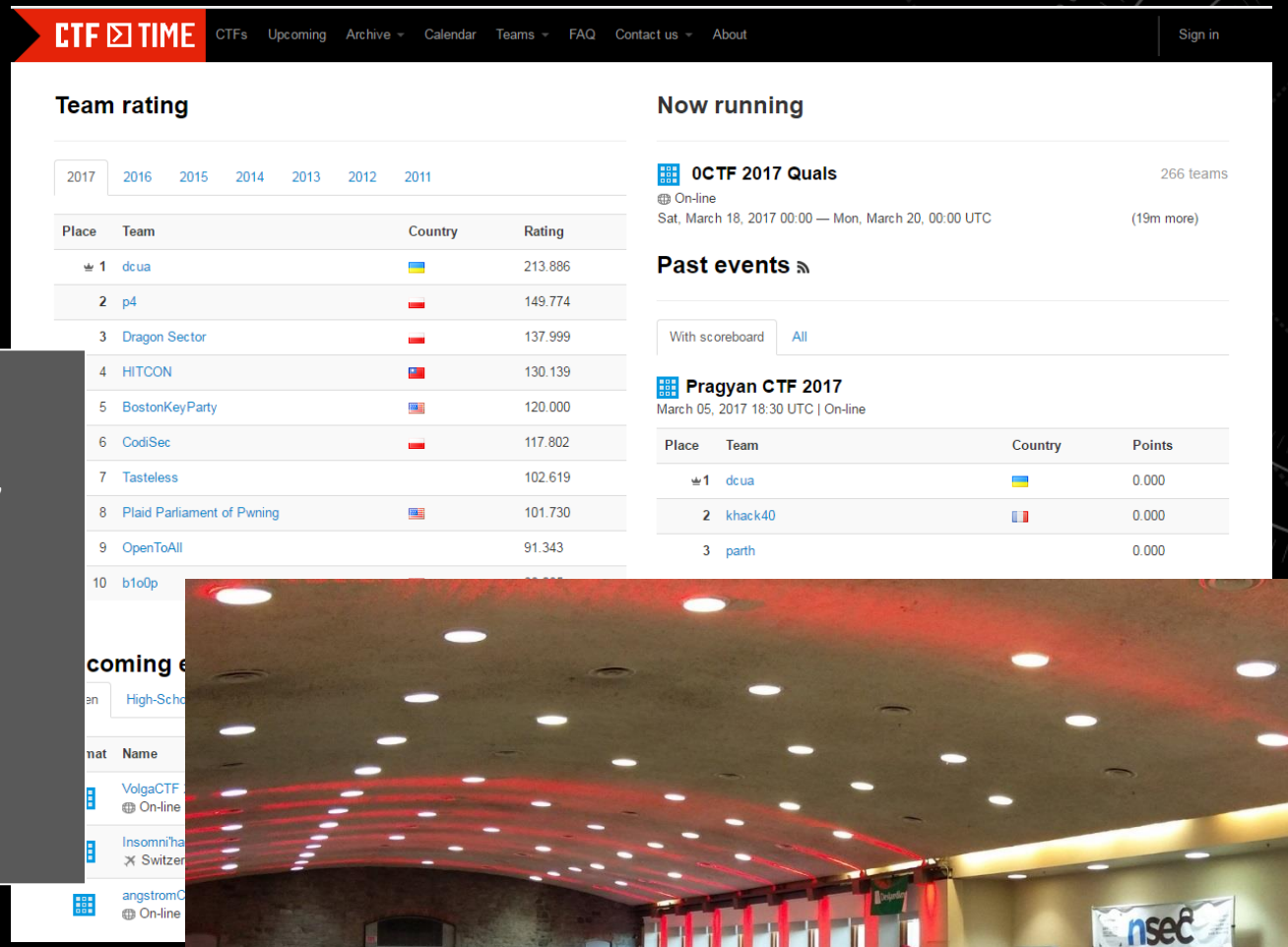
Multiple levels, going from easier to harder.

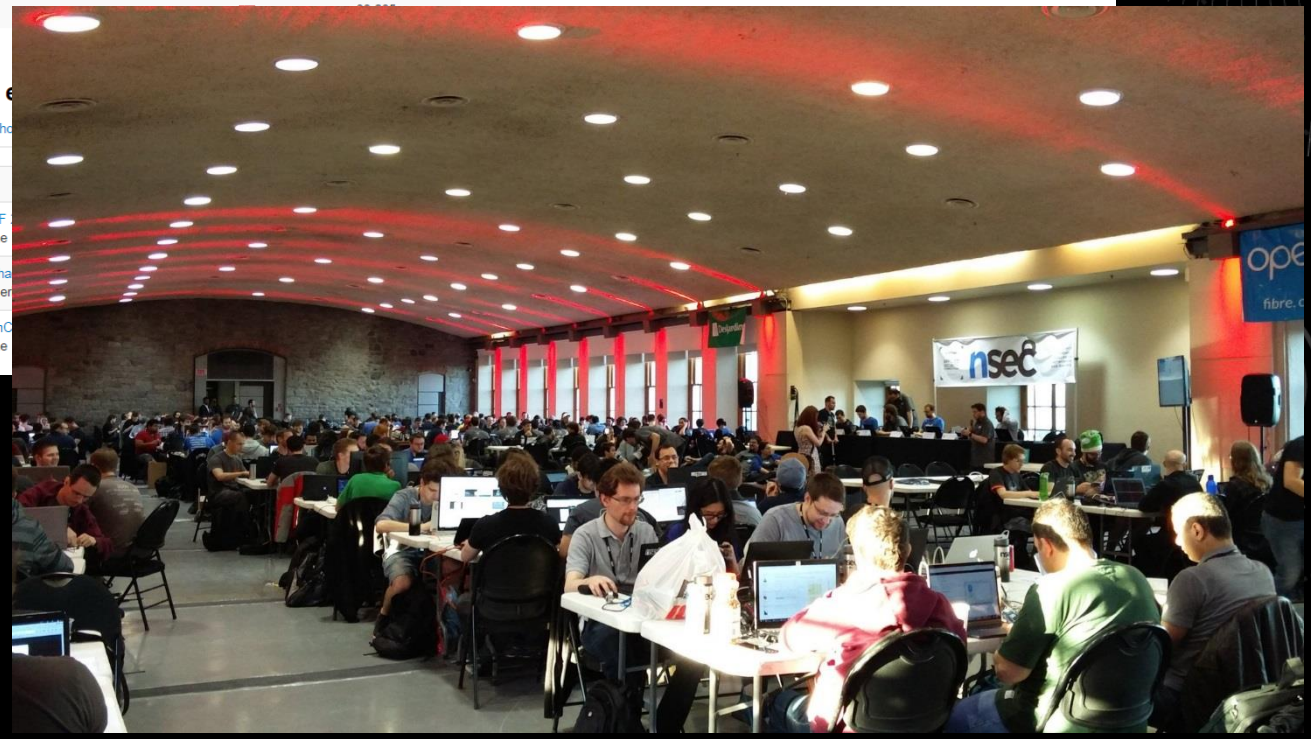
START HERE



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**



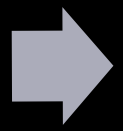


NSEC
Applied Security Competition in North America

A APPROACH FOR CTF WEB PROBLEMS

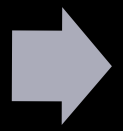
Reconnaissance

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



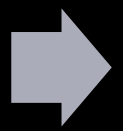
Mapping

- 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

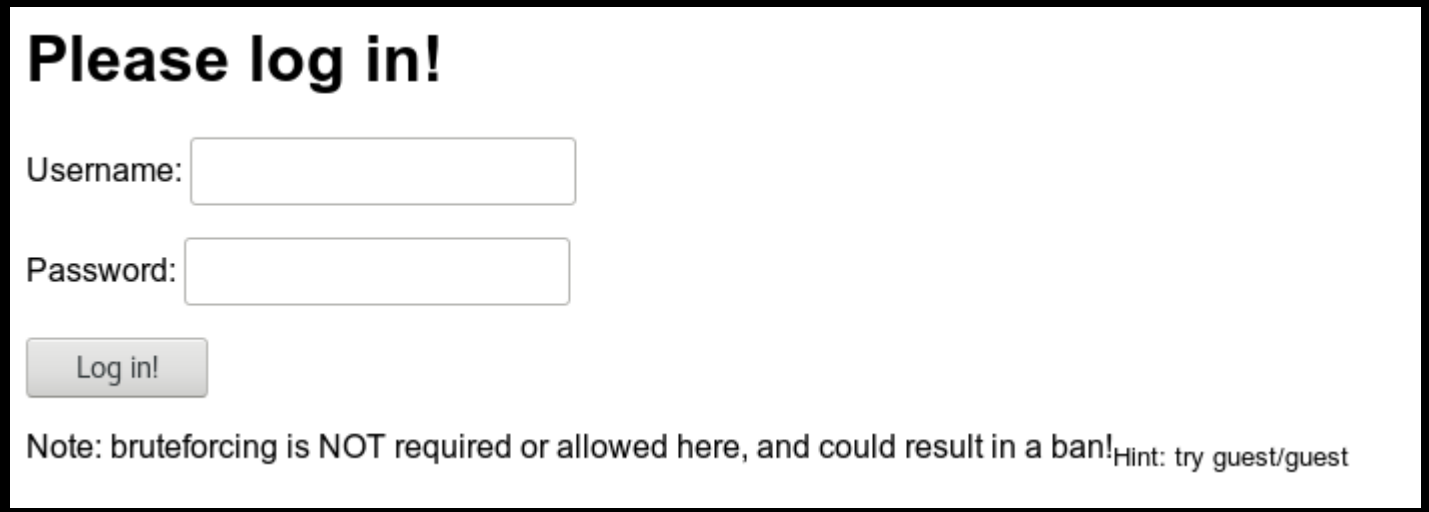
- Payload Construction
- Evasions
- Find the Flag!

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)

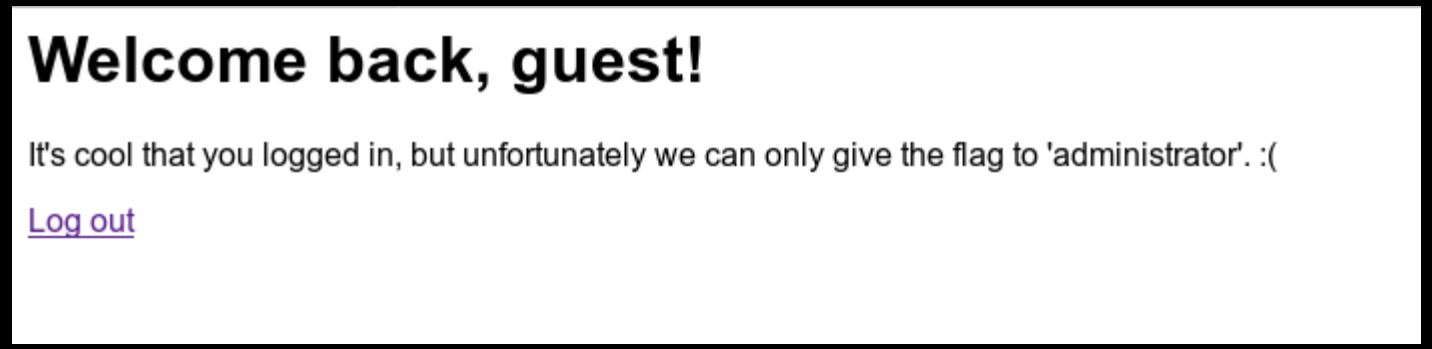
A BASIC 101 CHALLENGE – EASYAUTH

A CHALLENGE FROM BSIDESSF 2017

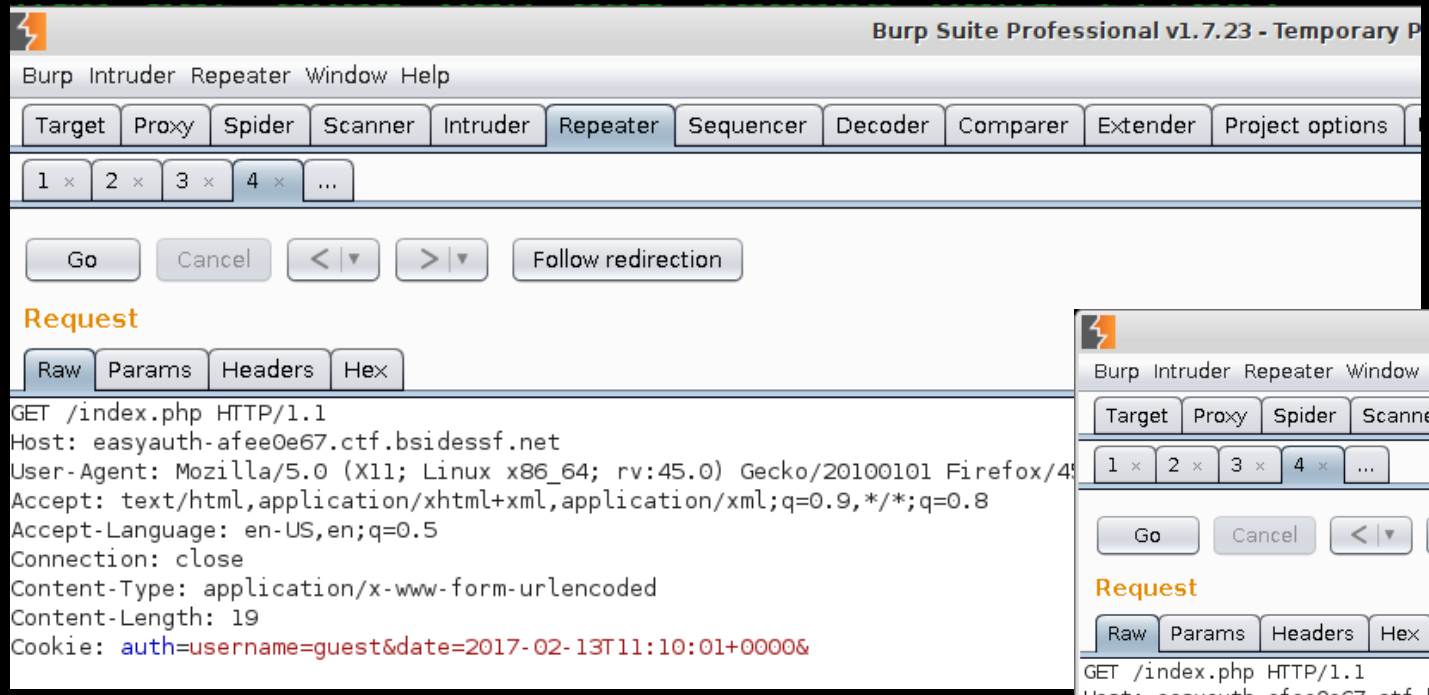


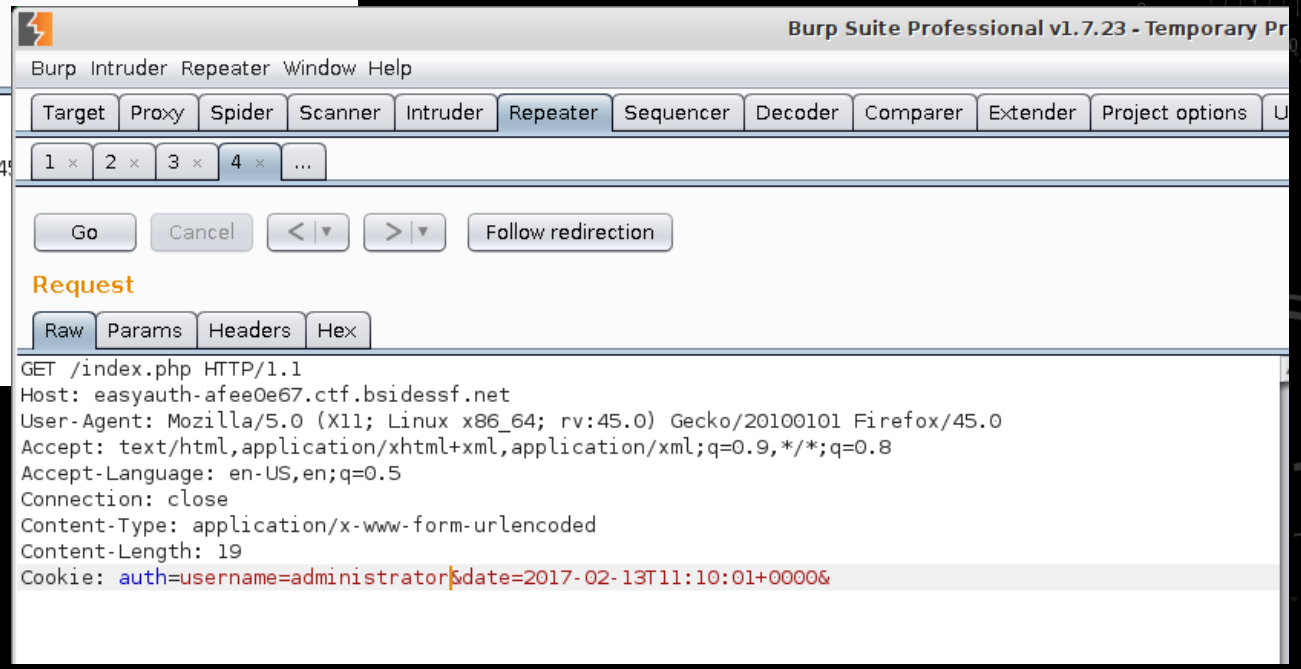
*Challenge from BsidesSF 2017

WARMING UP (EASYAUTH)

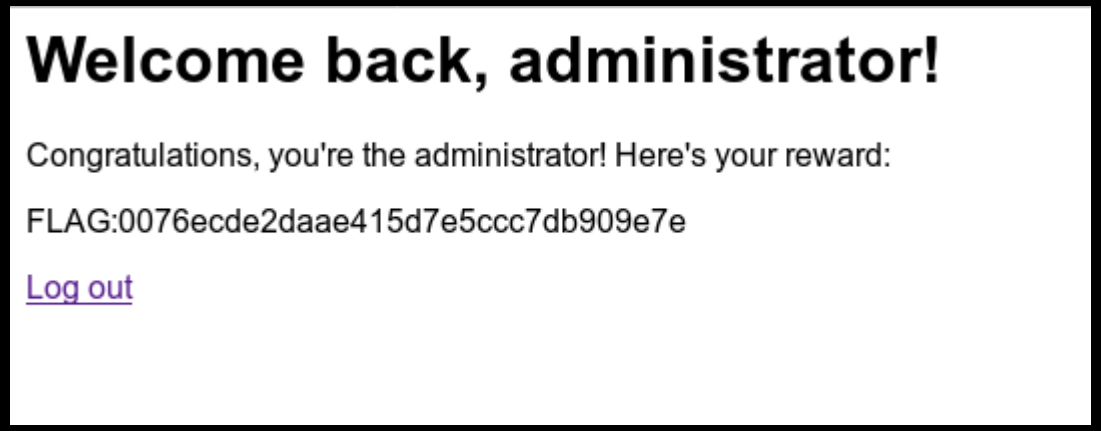


WARMING UP (EASYAUTH)





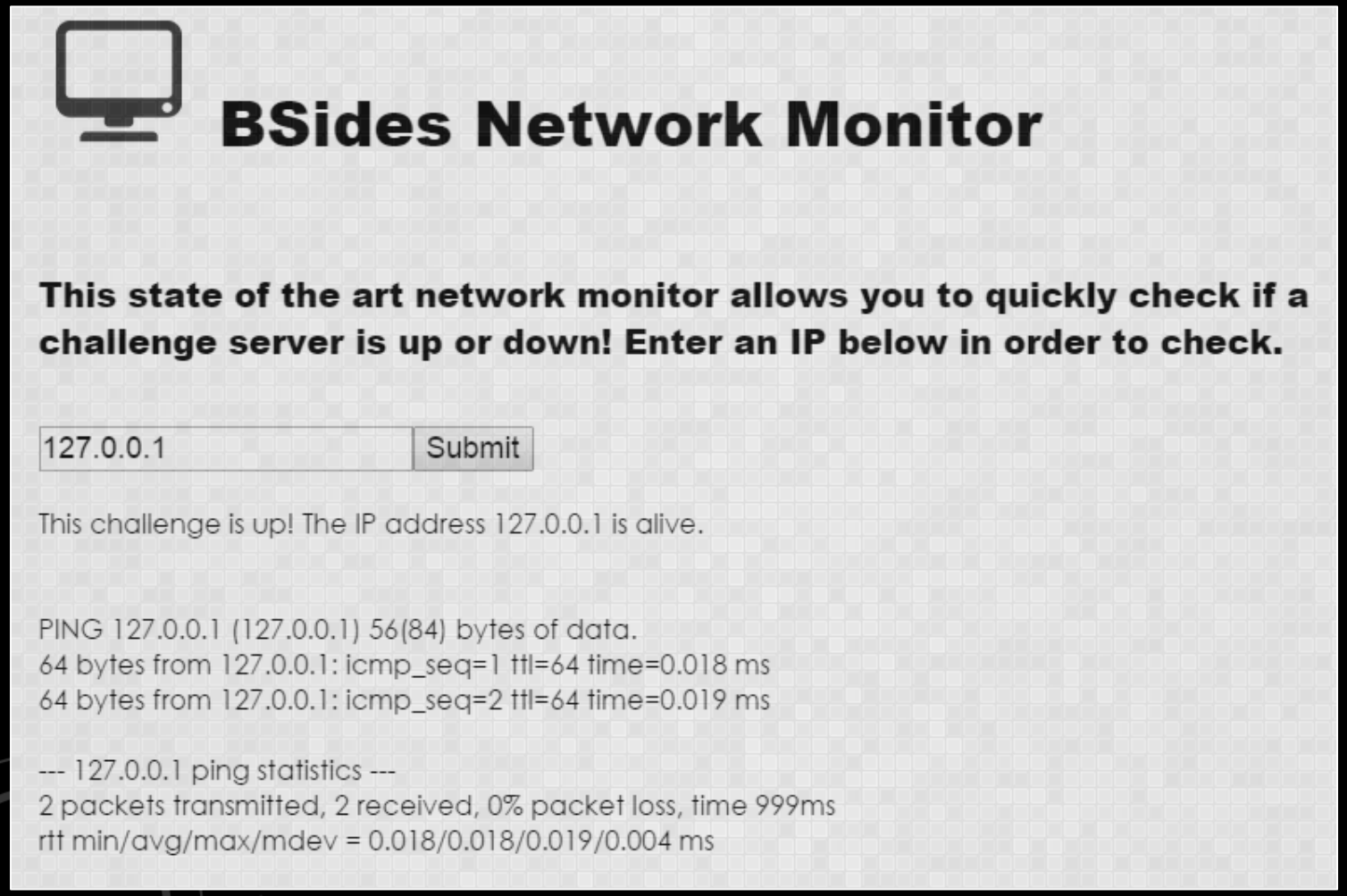
A BASIC 101 CHALLENGE



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

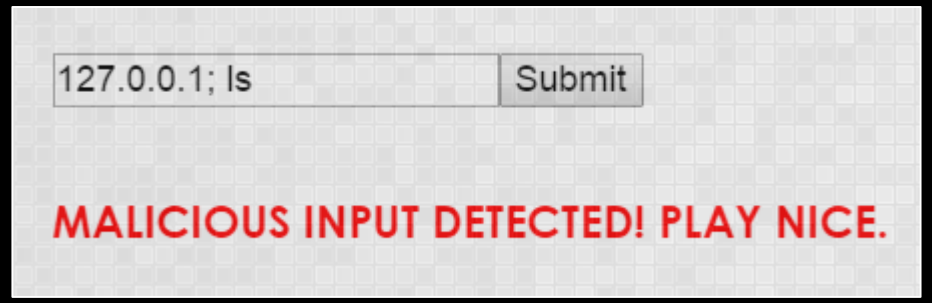
```
$cookie = $_COOKIE['auth'];

 $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

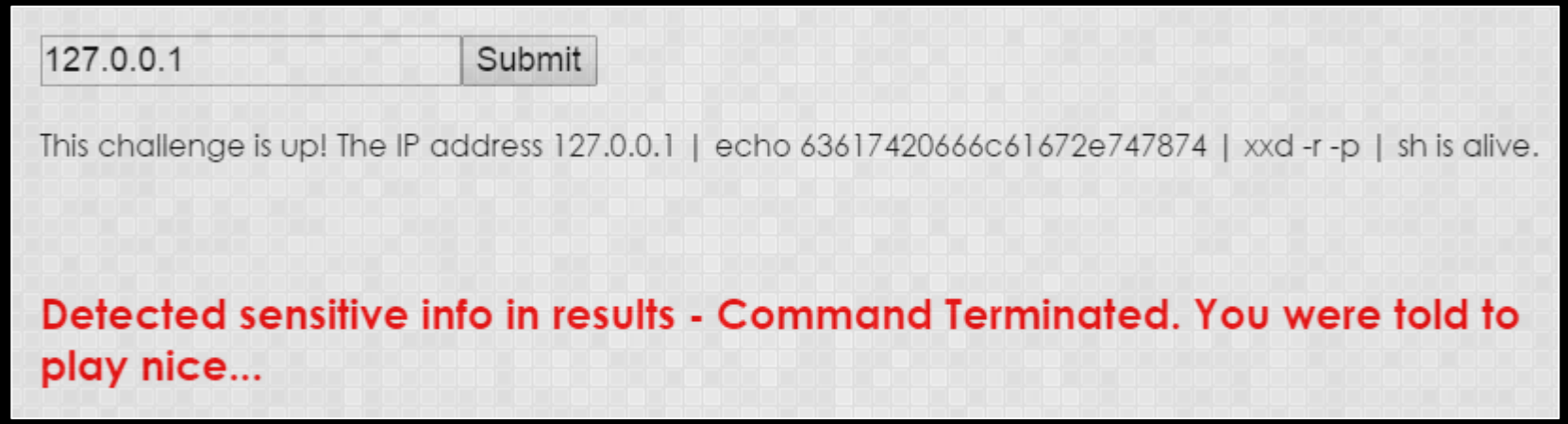


- Simple application to ping
- Two blacklist filters
- Several solutions possible

WEB200 – COMMAND INJECTION WITH FILTER

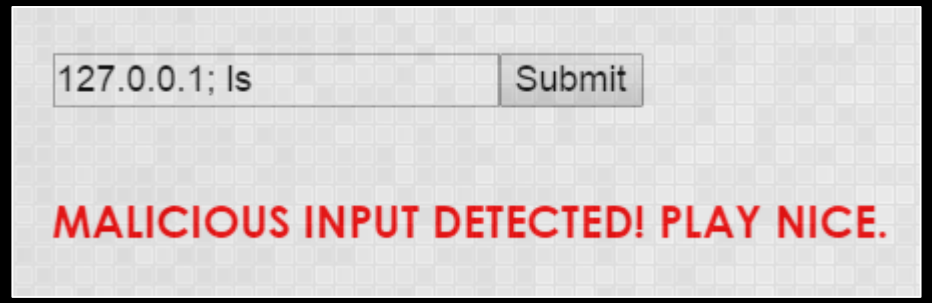


- Two filters:
  - Inbound commands filtered for the words/characters in $badwords
  - Outbound results filtered for the word 'FLAG' – OH NOES **DLP!**

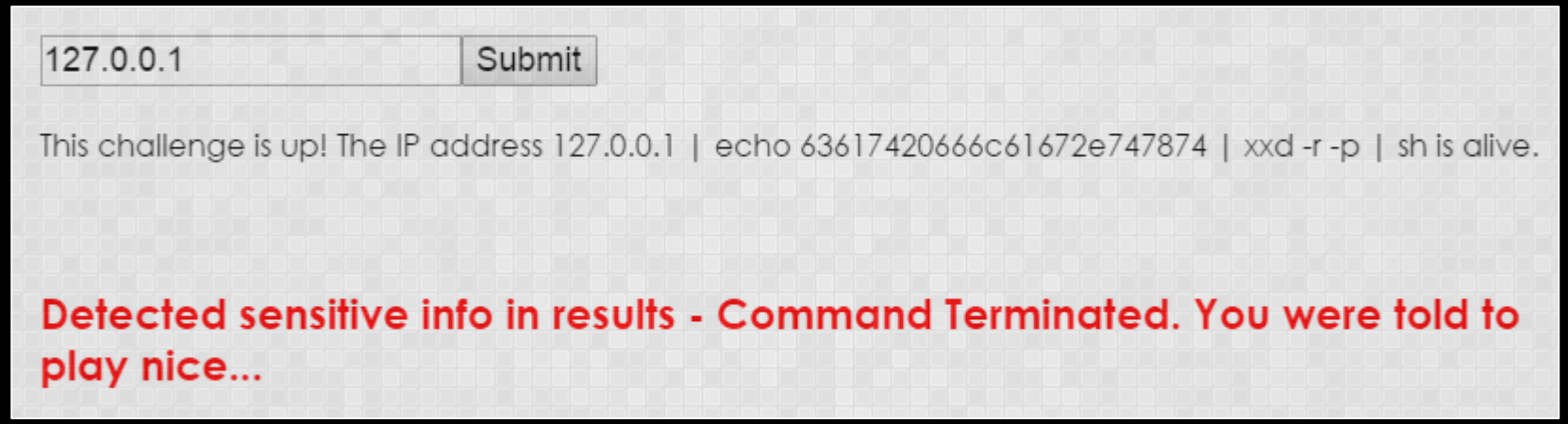



```
$badwords = array('cd','ls','cat','exec',';','&','more','file', 'head', 'less', 'od', 'tail', '$', '
xargs', 'print', '=','awk','grep','||', 'strings', 'binwalk');
```

WEB200 – COMMAND INJECTION WITH FILTER



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



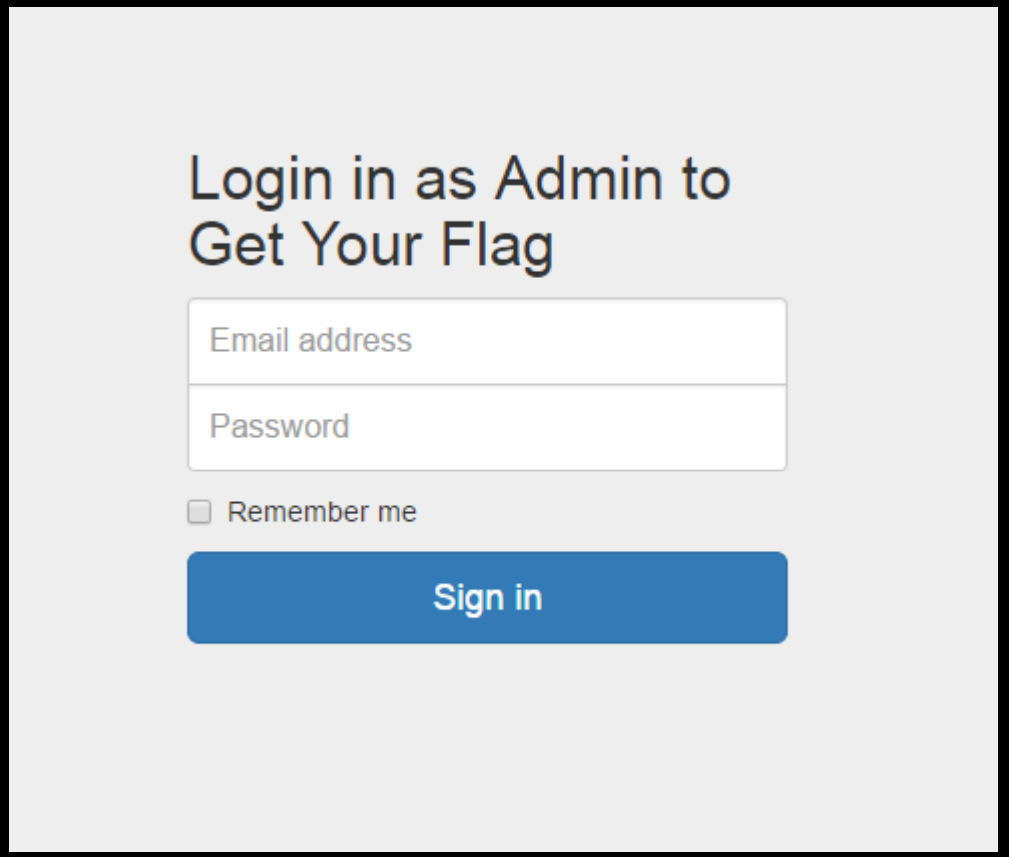

```
$badwords = array('cd','ls','cat','exec',';','&','more','file', 'head', 'less', 'od', 'tail', '$', '
xargs', 'print', '=','awk','grep','||', 'strings', 'binwalk');
```

WEB200 – COMMAND INJECTION WITH FILTER

- Intended Solution:

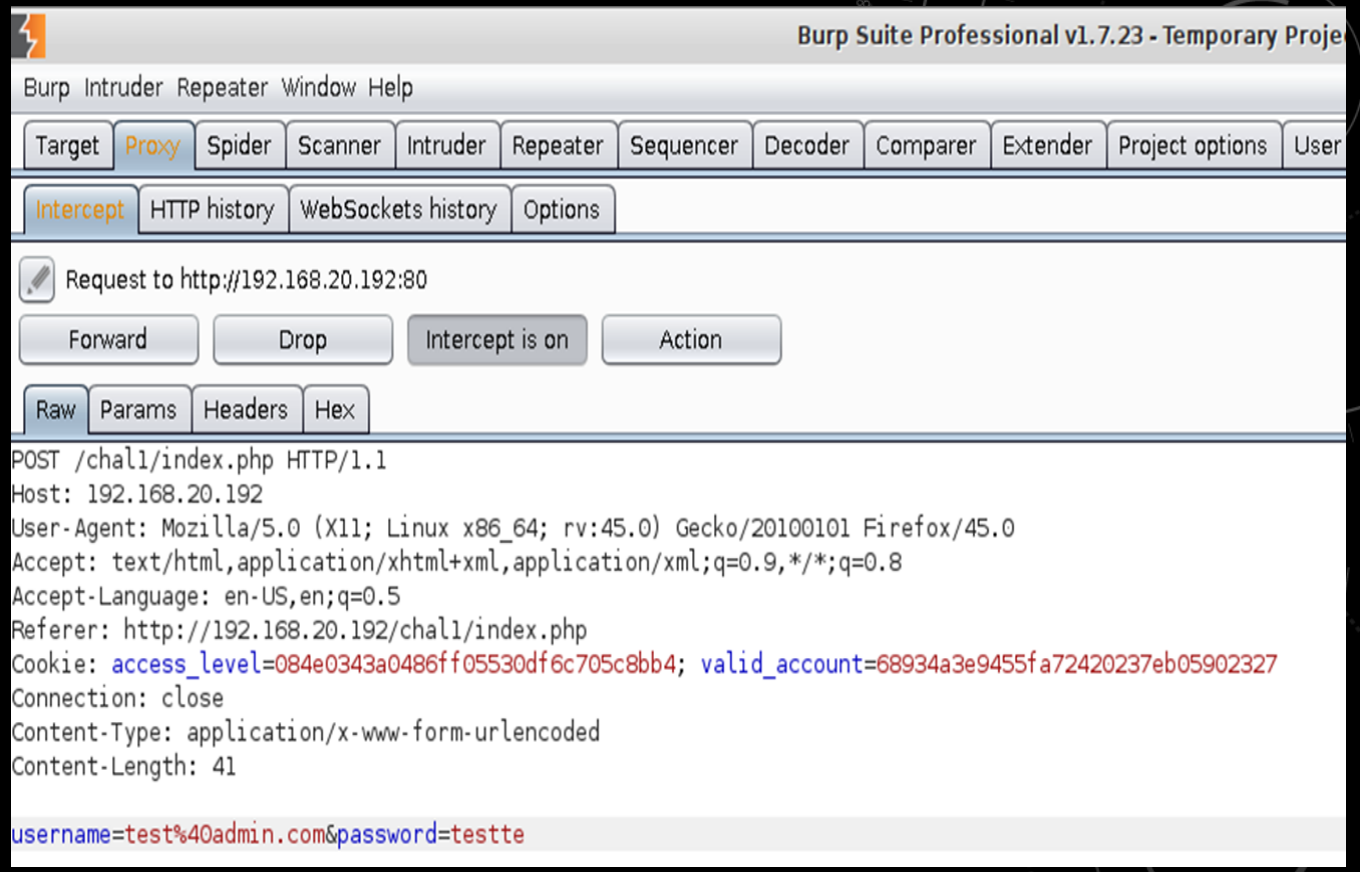
- The initial proof of concept for this challenge involved using a hexdump of the ‘cat flag.txt’ command and sending the decoded result to sh
- We saw different solutions than this

CHALLENGE #1 - REMEMBER ME?

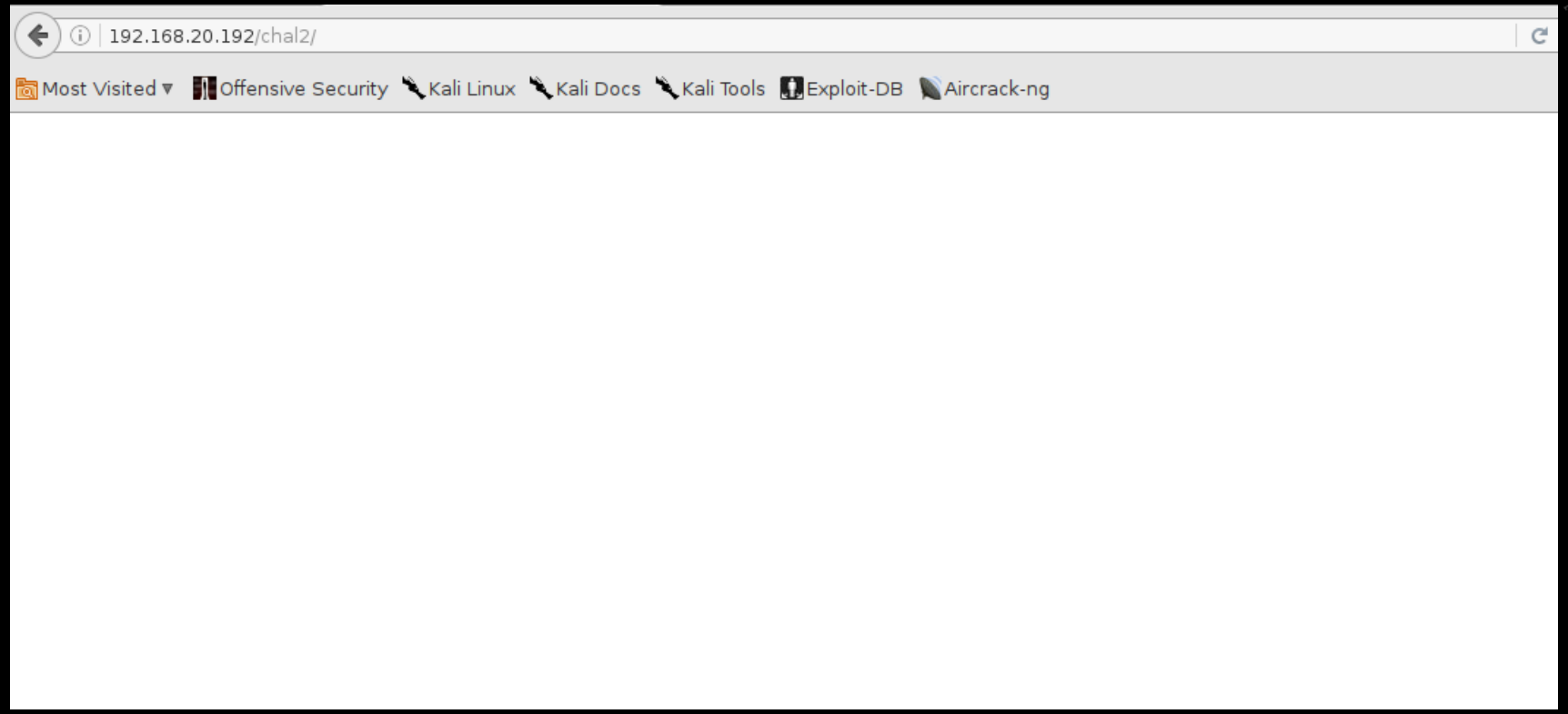


Intended Solution

- 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 privedges
- 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 redirecation 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

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