



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

Probably the **best CTF**
in Israel, EVER!



So, What did we have?

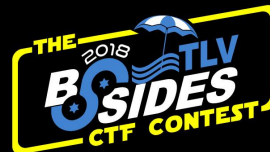
9 Members

no relation to bearers of the one ring, that's a different CTF

3 servers (sometimes 5)

19 Challenges in total

2 weeks, with challenges released almost every day



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

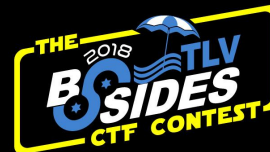
Feedback?

WE LOVE FEEDBACK!



וואו אחי אחד המעולים 17:51

תודה רבה על ההשקעה 17:51



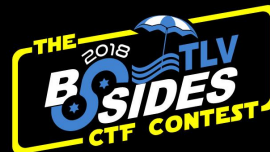


אתגר מדהים 15:49

לא ידעתי שספריות js יכולות להיות כאלה

דפוקות

15:50



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

רציתי רק להגיד מברוק על ה-CTF, אחת היותר
טובים שיצא לי להשתתף בהם, ובטח הישראלי הטוב
ביותר שראיתי.



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



There is one writeup that must be
written, and I don't care by whom:
wtflol

22:21



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

והחידה של reversing של ה 1000 נקודות
לאנשים בצוות נפל הלסת שהם הבינו מה הלך

שם

22:14



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Tue

You don't know how many times I've cursed you and wished you die, until I've solved wtflo_l_reflagged challenge (two minutes ago)

DIE DIE DIE!

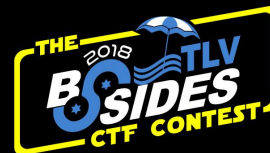
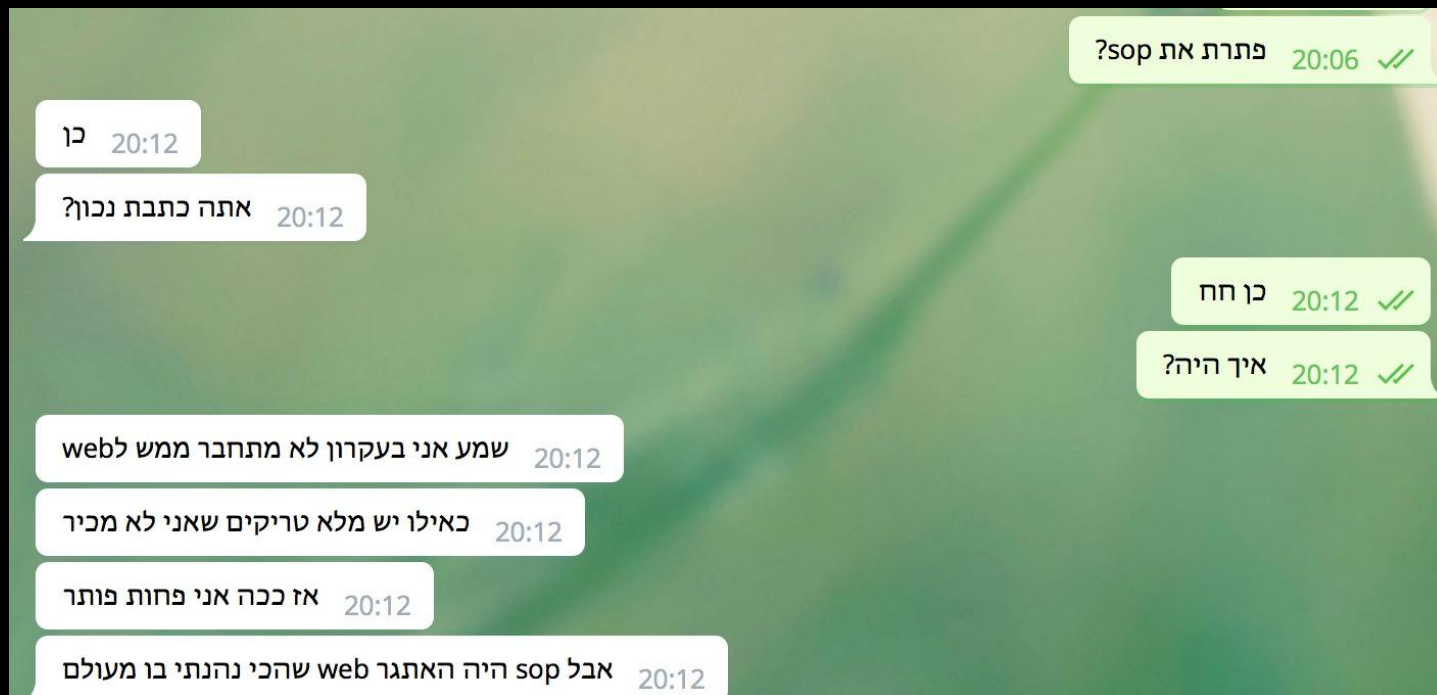
The 0x2D trick was unbelievable!
Undocumented ".ocommand"
for kernel.



```
bsidestlv@19554ce2b876:/var/run$ hello
hello
hello
any ideas?
nope
you?
the same
semek
maybe it is a key in \ and ssh to 172.18.0.1
interesting
but we need access to the private key file
ping
pong
is it just me, or they changed the container? it was writable earlier
i didnt figure ir out
im going home .... hope you will get an answer meanwhile twitter/gimpeltweet
^C
bsidestlv@19554ce2b876:/var/run$ clear

bsidestlv@19554ce2b876:/var/run$ cd ../../
bsidestlv@19554ce2b876:/ $ ls
app bin boot dev etc home lib lib64 media mnt opt proc root run s
bsidestlv@19554ce2b876:/ $ cd ~
bsidestlv@19554ce2b876:~$ ls
bsidestlv@19554ce2b876:~$ cd /var/run
bsidestlv@19554ce2b876:/var/run$ ls
docker.sock lock mount sshd systemd utmp
bsidestlv@19554ce2b876:/var/run$ hello
-bash: hello: command not found
bsidestlv@19554ce2b876:/var/run$ |
```





ומה יהיה שנה הבאה? זהו הצבתם רף גבוה

22:16

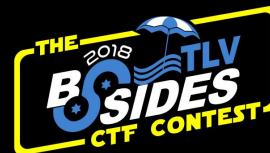
מפה אפשר רק לרדת 22:16

כלומר אם אתם לא תארגנו את ה CTF 22:16



ואני חייב להגיד לך שזה אחד ה ctf הכי ברמה
שהשתתפתי בהם

22:12



Really really impressed with
the quality of the CTF,
massive credit to the team
who built it.



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH





Tomer Zait

@realgam3



Please don't ask what challenge I like the most 😞 I feel like a father I can't choose between my children's, GamingStore (but don't tell the others 😂)

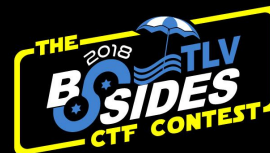
| | |
|--|------------|
| Topic | Game Store |
| Challenge: Shared Encryption, Redwood tree | 10/05/18 |
| Original: #10278643 | 10/05/18 |
| Blissware: Under the ocean back, Pongalphish | 10/05/18 |
| Amos: Can you escape me 10/17, 10/18/19 | 10/05/18 |
| Mr. Pongal: Back, Challenge 10/18/19 | 10/05/18 |
| Blissware: Amos: Can you escape me 10/17, 10/18/19 | 10/05/18 |
| Blissware: Amos: Can you escape me 10/17, 10/18/19 | 10/05/18 |
| Blissware: Amos: Can you escape me 10/17, 10/18/19 | 10/05/18 |

BSidesTLV_CTF @BSidesTLV_CTF

We are releasing our schedule for the rest of the CTF - 18 challenges, new ones (almost) every day!

12:41 AM - 5 Jun 2018

2 Likes



The Team Behind the Scenes



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Tomer Zait and Nimrod Levy

Tomer and Nimrod:

IAmBrute

Redirect me

IH8emacs

I'm Pickle Rick!

Creative Agency

ContactUs

Tomer:

c1337Shell

DockingStation

PySandbox-Insane

GamingStore

Nimrod:

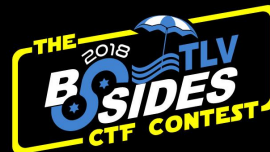
Shared Directory

Can you bypass the
SOP?

NoSocket



SCORPIONES



Guy, Adir, Omer and Kasif

Guy Barnhart-Magen:

Crypto2

T.A.R.D.I.S.

Adir Abraham:

Into the rabbit hole

Gal Goldstein:

PimpMyRide

Omer Agmon:

hideinplainsight

Kasif Dekel:

WTFLOL (and wtflool_reflagged)

More on that later

Ido Naor, Ezra Caltum and Omer Cohen:

Advice and support, as well as QA :-)



Transparency and Incident Handling

WTFLOL had the **flag leaked**, accidentally

We made a decision to **keep the challenge**, but modify the flag
(WTFLOL_reflagegd)

We **didn't disqualify** the parties involved, but we were **very close to do so**

We **disclosed the entire affair**, and our thinking on the CTF site

Please play fairly! both for your sake, and for the fun of everyone else!

<https://ctf18.bsidestlv.com/FairGame>



Dedicated SOC and IT Support: 24/7

Keeping a system up and running - with active hacker engagement isn't easy

Many sleepless nights...



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Dedicated SOC and IT Support: 24/7

Keeping a system up and running - with an active hacker engagement isn't easy

Many sleepless nights...



Statistics



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Amazing Participation!

312 teams registered

112 solved at least one challenge

1275 unique IP addresses

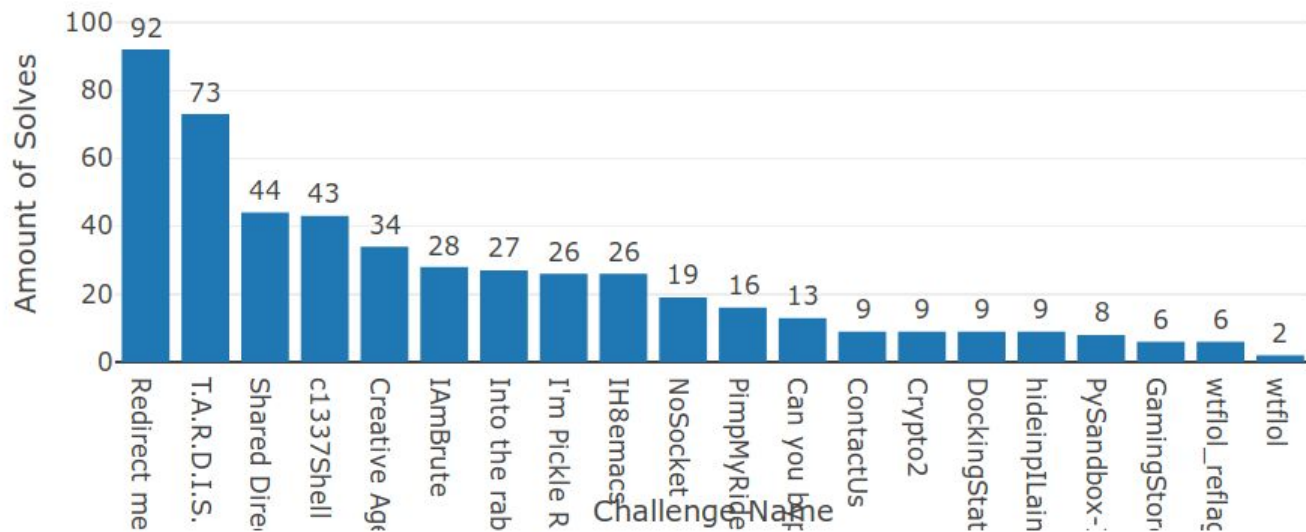


ctf18.bsidestlv.com

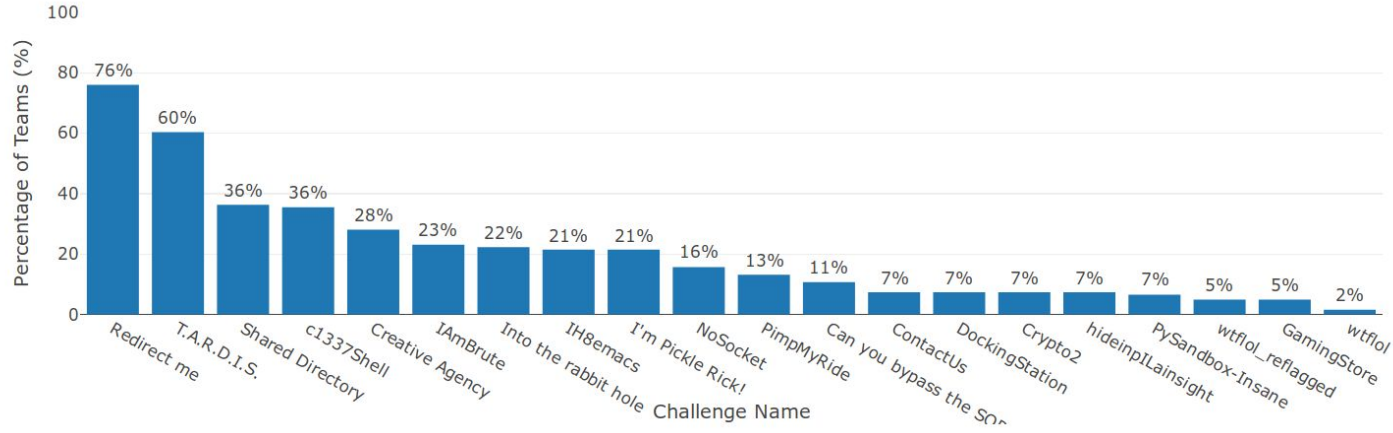
CONTEST JUNE 4TH-17TH



Solve Counts



Solve Percentages per Challenge



And the Winners are...



3rd Place:

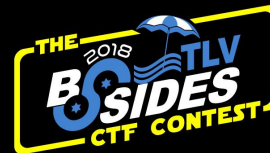


ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Team: _JCTF_



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



2nd Place:



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Team: babyr00t



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



1st Place:



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



Team: doadam

From Amsterdam,
solving all
challenges first!

@doadam



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

Team: reclass



ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



We had a lot of fun doing this!

Come chat with us, give us some **feedback**!

We plan on releasing the challenges on **GitHub** and on **VulnHub**

Call for write-ups: **please send us your write-ups** so we can share! (ctf@bsidestlv.com)

We plan on doing a write-up of the CTF process itself, to be released soon

Follow us on twitter for more updates: **@BSidesTLV @BSidesTLV_CTF**

See you next year, and may the force be with you!

