ctf18.bsidestlv.com

Contest June 4th-17th

Probably the best CTF in Israel, EVER!

ctf18.bsidestlv.com

Contest June 4th-17th

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

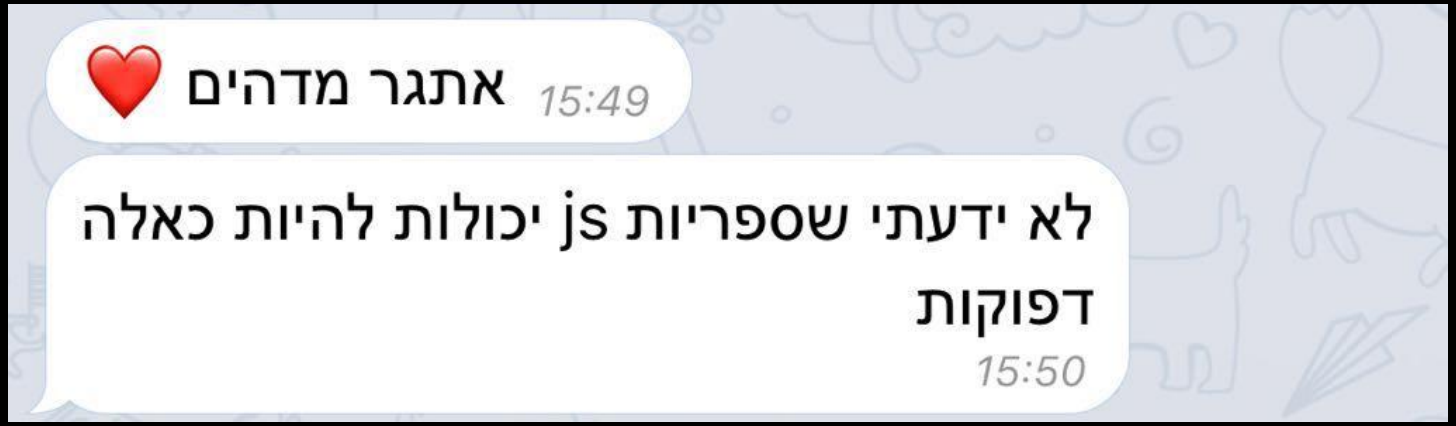
Feedback?

WE LOVE FEEDBACK!

ctf18.bsidestlv.com

Contest June 4th-17th

THE 2018 TLV BSIDES CTF CONTEST
ctf18.bsidestlv.com
Contest June 4th-17th

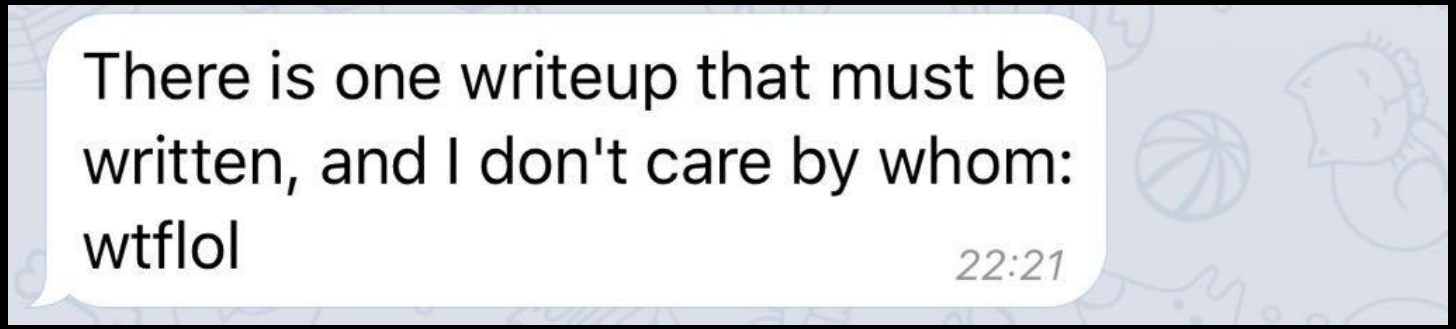


THE BSIDES TLV 2018 CTF CONTEST
ctf18.bsidestlv.com
Contest June 4th-17th

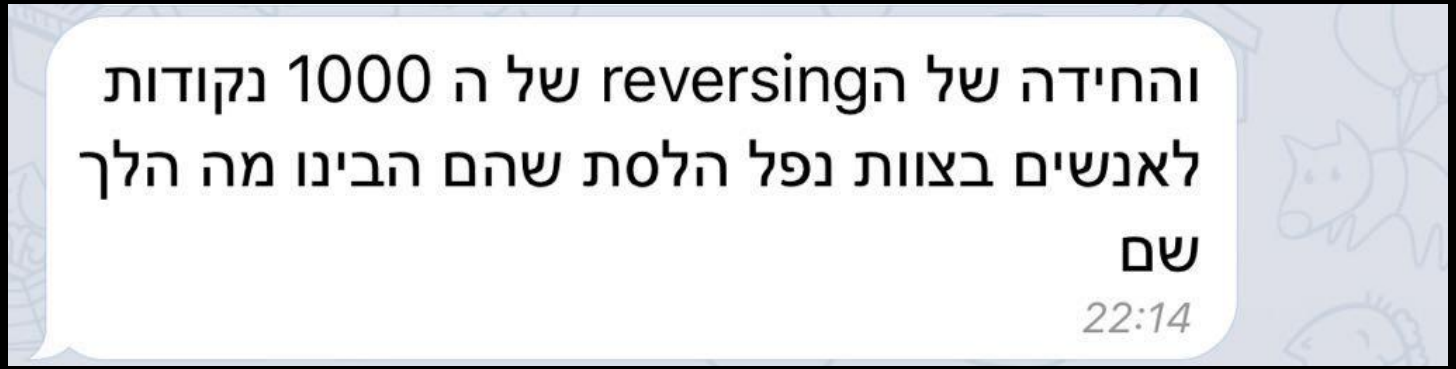
רציתי רק להגיד מברוק על ה-CTF, אחת היותר טובים שיצא לי להשתתף בהם, ובטח הישראלי הטוב ביותר שראיתי.

ctf18.bsidestlv.com

Contest June 4th-17th



THE 2018 BSIDES TLV CTF CONTEST
ctf18.bsidestlv.com
Contest June 4th-17th



THE 2018 BSIDES TLV CTF CONTEST
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 wtflol_reflagged challenge (two minutes ago)

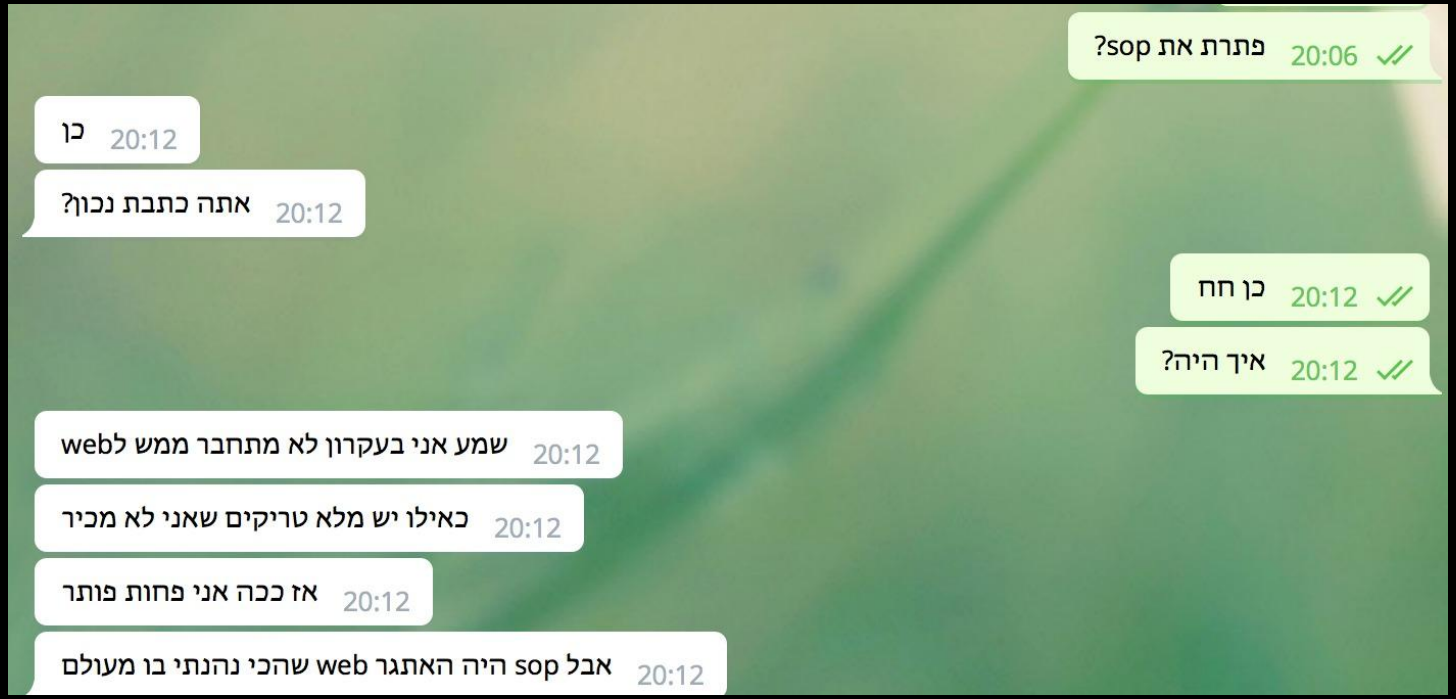
DIE DIE DIE!

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

THE 2018 BSIDES TLV CTF CONTEST
ctf18.bsidestlv.com
CONTEST JUNE 4TH-17TH

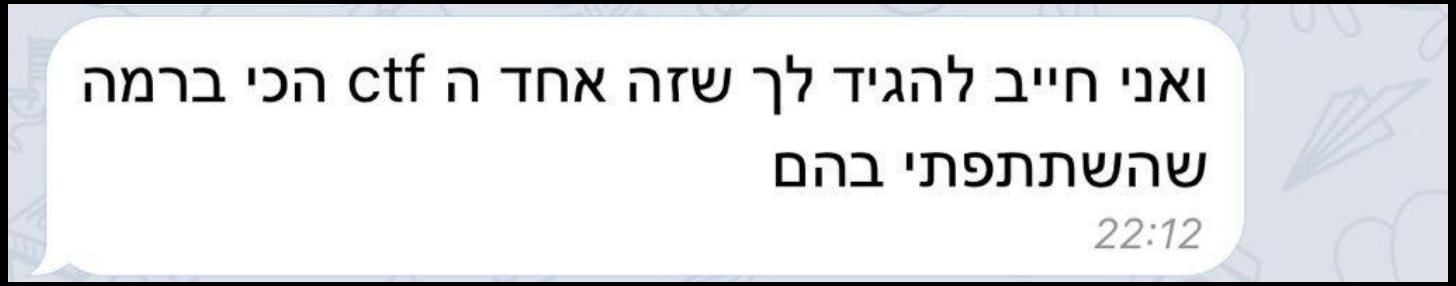
```
bsidestlv@19554ce2b876:/var/run$ hello
hello
hello
any ideas?
nope
you?
the same
semek
maybe it is a key in \ and ssh to 172.18.0.1
interesting
but we need access to the private key file
ping
pong
is it just me, or they changed the container? it was writable earlier
i didnt figure ir out
im going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

THE 2018 BSIDES TLV CTF CONTEST
ctf18.bsidestlv.com
CONTEST JUNE 4TH-17TH



THE 2018 BSIDES TLV CTF CONTEST
ctf18.bsidestlv.com
Contest June 4th-17th

THE 2018 BSIDES TLV CTF CONTEST
ctf18.bsidestlv.com
Contest June 4th-17th

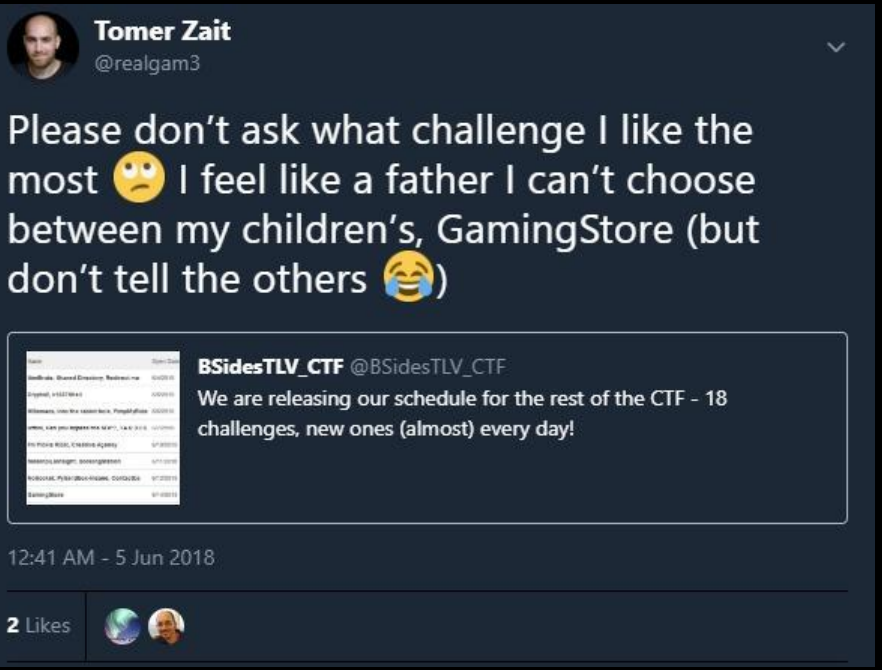


THE 2018 TLV BSIDES CTF CONTEST
ctf18.bsidestlv.com
Contest June 4th-17th

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

ctf18.bsidestlv.com

Contest June 4th-17th



THE 2018 BSIDES TLV CTF CONTEST

ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

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

ctf18.bsidestlv.com
Contest June 4th-17th

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:
hideinplLainsight

Kasif Dekel:
WTFLOL (and wtflol_reflagged)
More on that later

Ido Naor, Ezra Caltum and Omer Cohen:

Advice and support, as well as QA :-)

ctf18.bsidestlv.com
Contest June 4th-17th

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

ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

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!

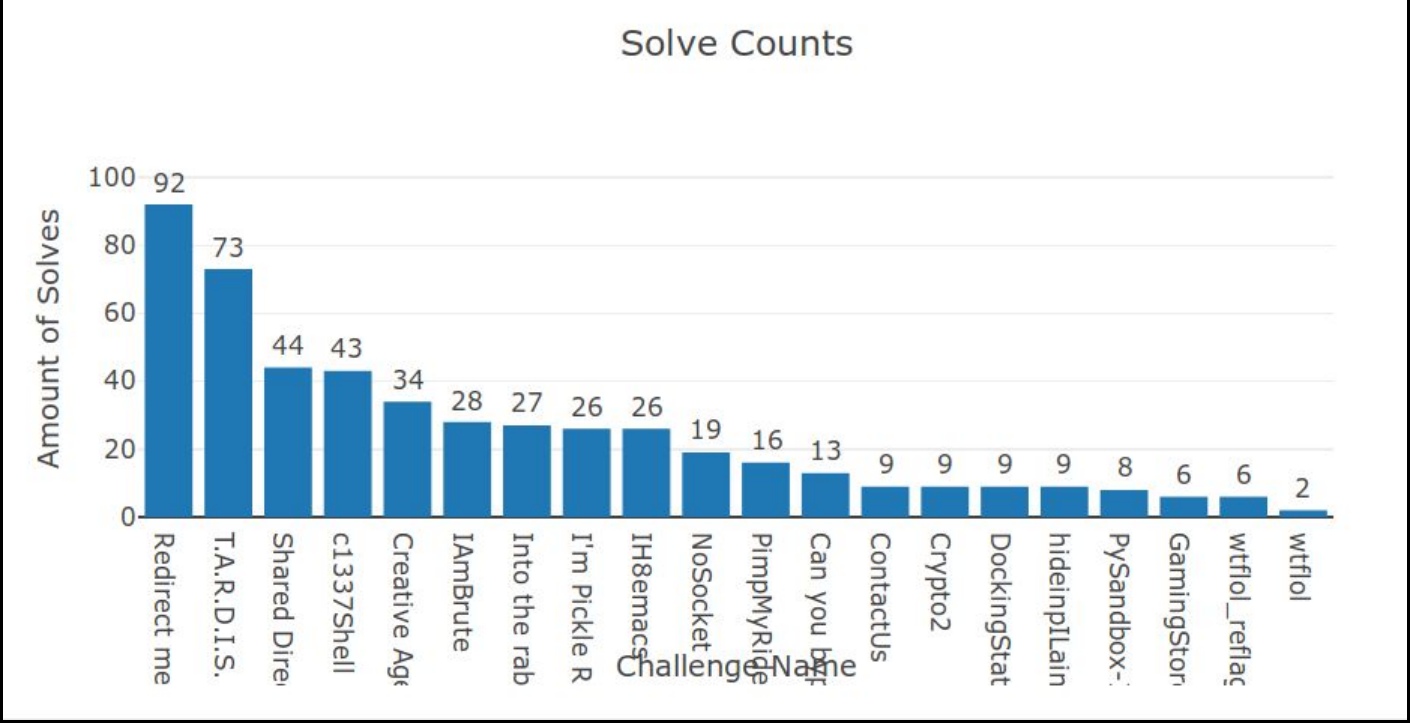
312 teams registered

112 solved at least one challenge

1275 unique IP addresses

ctf18.bsidestlv.com

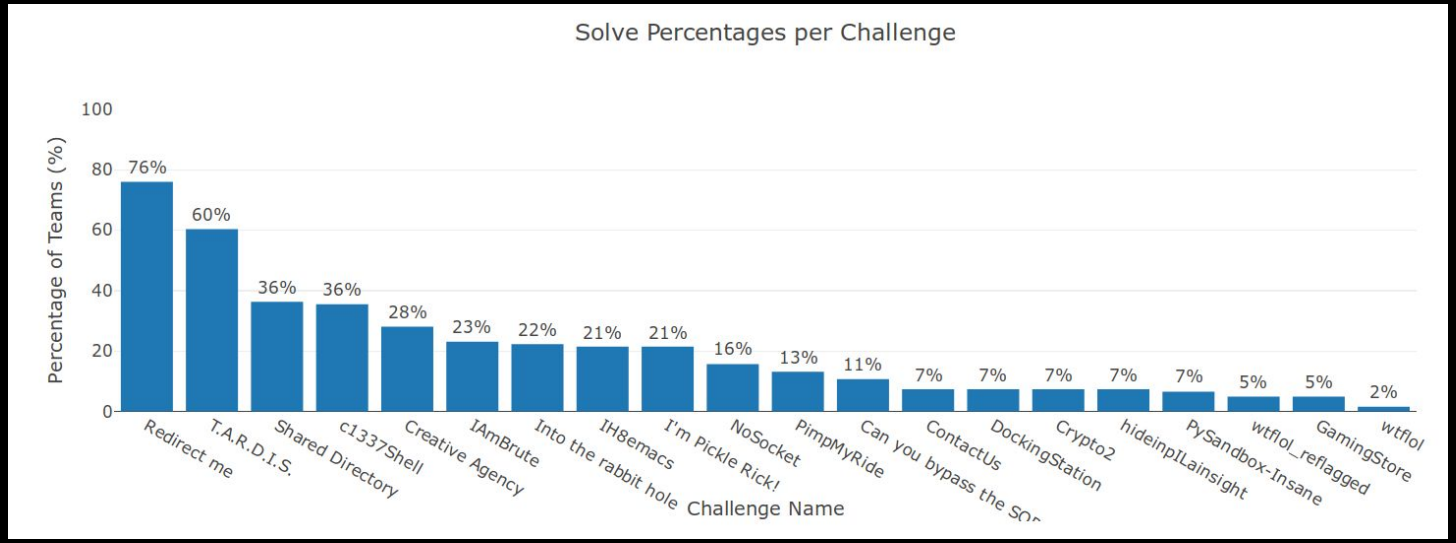
Contest June 4th-17th



THE BSIDES TLV 2018 CTF CONTEST

ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH



THE 2018 BSIDES TLV CTF CONTEST

ctf18.bsidestlv.com

CONTEST JUNE 4TH-17TH

And the Winners are...

ctf18.bsidestlv.com

Contest June 4th-17th

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

THE 2018 BSIDES TLV CTF CONTEST
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!

ctf18.bsidestlv.com

Contest June 4th-17th