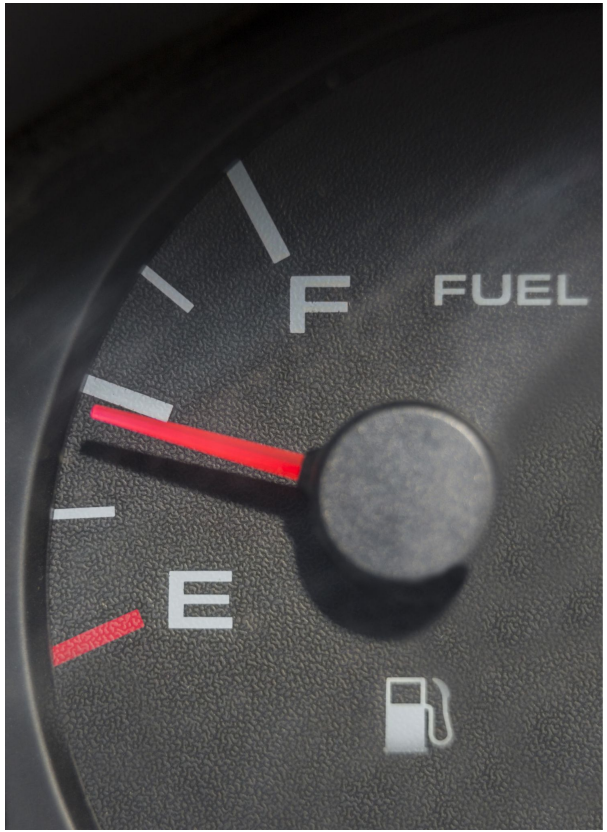
Kiber-sprīdītis: Manas pirmās 200 stundas ar Bug Bounty

Autors: Gvido Bērziņš (Cny)



Ir iemesls kāpēc “pirmās 200 stundas”

Alternatīvie prezentācijas nosaukumi

Kam es nebiju gatavs sākot bug bounty?

Ieteikumi no minimāli kompetenta hakera

Slikta prakse sākot bug bounty

Ko profiņi teica, lai nedara sākot bug bounty un ko es tāpat dariju un “wow, tas arī nestrādāja”

Kas te? Es te!

- Gvido Bērziņš (“Cny”, es nezinu kā izrunā, “cīnis”, “cinijs”?)
- Programmatūras testētājs un izstrādātājs, lektors, kiberdrošības speciālists
- Papīri: Foundation ISTQB, OSCP 😏
- Sadarbības partneris CITM Advisory
- Sports: lelu vingrošana, snowboarding, daiļslidošana, bouldering

Mani bug bounty pirmsākumi un sākumi

Pirms sākam par bug bounty

- Interesējos par kiberdrošību no 2021. gada.
- Uzzināju par bug bounty 2023. gadā?
- Aizgāju no darba Aprīlī.
- Sāku kaut ko beidzot sākt darīt Jūnijā.

Ar ko es sāku?

- Hackerone un Hacker101.
- Arī izskatīju Bugcrowd, Intigiriti un YesWeHack.
- Pirmā programma: DIB-VDP.
- Lielākoties “recon” (novērošanu).

Kā man tur gāja sākumā?

- Slikti :)
- Nezinu, ko darīt, bet mēģinu visu.
- Demotivācija, garlaicība, slinkums un stress.

Kas tālāk?

- Bija jāpaņem daži soļi atpakaļ.
- Mācības un pētījumi.
- Varbūt cits VDP vai BBP?

Atskats uz Jūniju

Jūnijs

- Pirmais VDP
- Atpakaļ mācīties
- Nedaudz skila atsvaidzināšana
- Noderīgi atradumi:
  - Critical Thinking - Bug Bounty Podcast
  - Sticking With It: How To Choose a Target & Stay Motivated - w/Katie Paxton-Fear (@InsiderPhD)
  - Bug Bounty Reports Explained

“Ražīgāks” Jūlijs

Jūlijs

- Pirmā privātā BB programma (Intigriti)
- Pirmais ievainojamību atskaite
- BB programmu lēkāšana

Pirmā ievainojamība?


changed the status from Triage to Not applicable

Emocijas

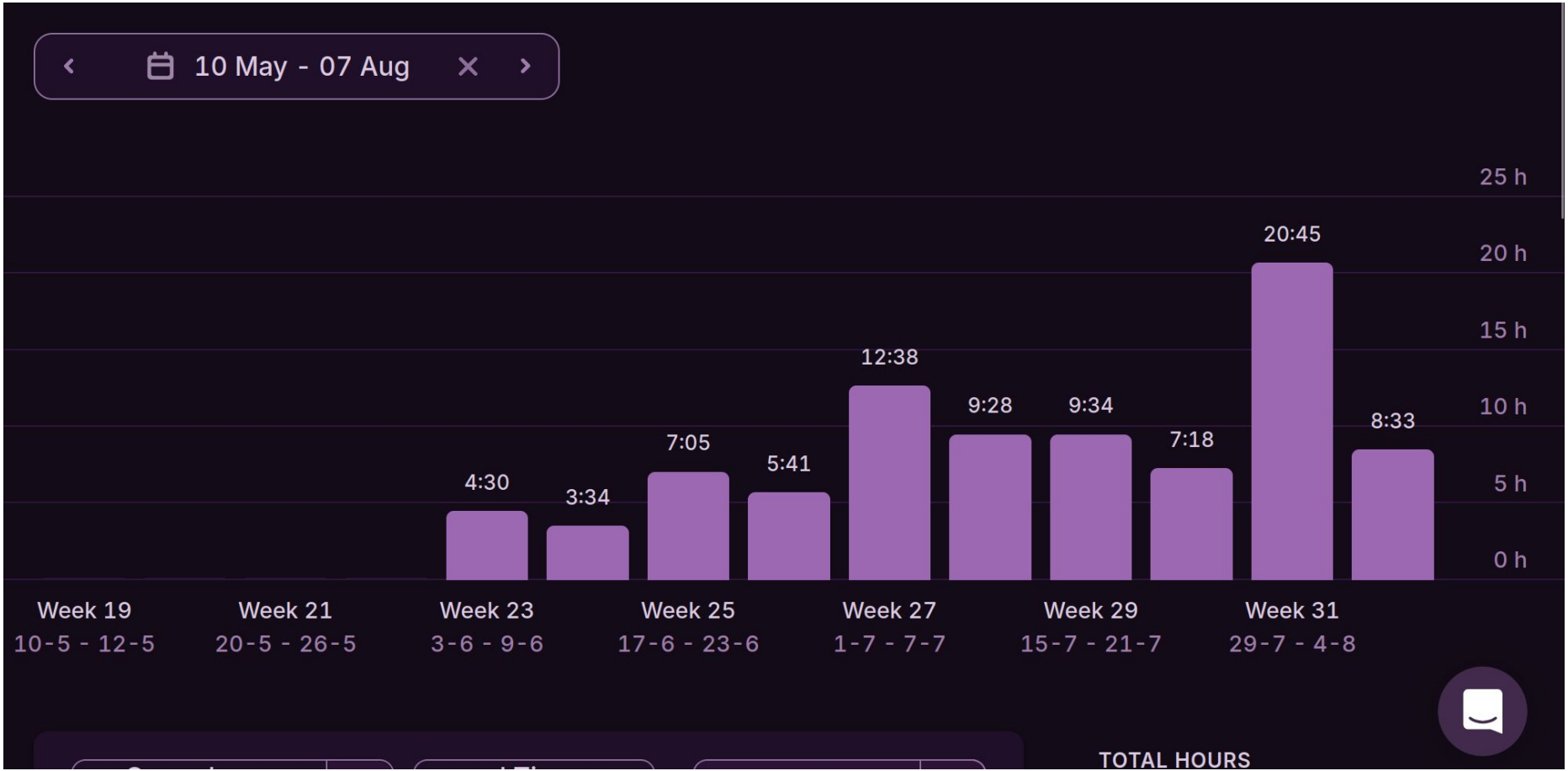
- Eh... 50/50
- Jaunu programmu sākt vienmēr jautri.
- Kamēr neatradu motivātoru, ātri apnika programmas.

Augusta sākums un nākamie plāni

Augusts

- Divi jauni ielūgumi YesWeHack platformā
- Plānošana un plānošana
- Kārtīgāka programmas izskatīšana un izvērtēšana
- Citas atklāsmes un apgaismības

Atskats atpakaļ uz noieto ceļu


10 May - 07 Aug
25 h
20 h
15 h
10 h
5 h
0 h
4:30
3:34
7:05
5:41
12:38
9:28
9:34
7:18
20:45
8:33
Week 19
10-5 - 12-5
Week 21
20-5 - 26-5
Week 23
3-6 - 9-6
Week 25
17-6 - 23-6
Week 27
1-7 - 7-7
Week 29
15-7 - 21-7
Week 31
29-7 - 4-8
TOTAL HOURS

Secinājumi

- Ir vajadzīgas kārtīgas robežas un disciplīna
- Jāatrod “īstā” programma vai ievainojamību tips
- Jāturpina mācīties un pētīt

Ko būtu labāk darijis?

- Palicis pie vienas programmas ilgāk
- Izskatijis un novērtējis katru programmu ilgāk
- Palicis pie viena ievainojamības tipa
- Pielietojis motivācijas hakus
- Sasniedzami mērķi
- Vairāk lasijis publiskās atskaites
- Novērtējis savu laiku un ieguldijumu

Vai es turpināšu?

Protams.

Resursi un ieteikumi

Pelnīšana no BB Latvijā

- Pašnodarbinātas personas noteikumi
- Bezdarbnieka pabalsts vēljoprojām tiek iegūts līdz ienākumi nepārsniedz 700 EUR mēnesī
- Intigriti, YesWeHack visvieglāk ir tikt galā ar KYC

Ievainojamību atrašana

- Noteikti jābūt kaut kādai ievainojamībai, kas visvairāk interesē
- Domā kā izstrādātājs, izmēģini laboratorijas, pats uztaisi kaut ko līdzīgu
- Mēģini salauzt mērķi (atrodi “un-happy path”)
- Pārbaudi vai dokumentācijā sacītais ir patiess
- Meklē jaunas fīčas (support, FAQ, stackoverflow, newsletter, blog)
- Izvēlies programmas ar sadalītu atļauju modeli un/vai plašu “scope”
- JS faili ir Tavi draugi
- Centies atrast sliktāko gadījumu ar ievainojamībām

Kas varētu būt man mīļākās ievainojamības?

Kas padara medības jautrākas un motivācija

- Ievainojamību tips
- Ekspertīze
- Produkts, kas interesē
- Sadarbība ar citiem
- “Cliffhangers”
- Pašizveidots grafiks
- Katrs var atrast savu motivāciju

Populārie urķi un iedvesmu avoti

- Nahamsec, Jason Haddix, Zseano
- Critical Bug Bounty podcast
- Hakeru intervijās var atrast iespaidīgus cilvēkus
- Visu ko atrodi konferenču ierakstos

Kur varu hakot?

Medību lauki

Iztestēti:

- **Intigriti**
- **YesWeHack**
- Hackerone

Nākamie rindā:

- Bugcrowd
- SynAck

Citas platformas

- **CVD Platforma** (https://cvd.cert.lv/programs/all)
- Code4rena - smart contracts
- CodeHawks - smart contracts
- Immunefi - smart contracts
- Remedy - smart contracts
- Sherlock - smart contracts
- **BugBase**
- HackenProof - smart contracts
- Standoff365 - krievijā bāzēta platforma

https://bbradar.io/ - ko izmantoju atradumiem

Vēl noderīgi

- Reģistrēties un lasīt noteikumus par privātajām programām
- Naudas izmaksas (*ahem, es maksātu nodokļus)
- Meklēt programmas manuāli
  - https://github.com/sushiwushi/bug-bounty-dorks
  - site:*.lv intext:“bug bounty”
  - “bug bounty program”
  - “vulnerability disclosure program”

Ko vēl varu ieteikt

- Izvēlēties platformas, kurās mazāk cilvēki hako
  - Vairāk iespēja uz ielūgumiem
- Izvēlēties eiropā dibinātu platformu
- Iesniegt jebkādu atskaiti, ja ir atradums un novērtēt komandas komunikāciju

Ieteikumi uzsākot bug bounty

- Pārliecinaties vai ir **stabili ienākumi**
- Pusslodzes bug bounty hunting ir arī iespēja
- **Atceries!** Izmaksas ir atkarīgas no programmas un no cilvēkiem
- **Have fun!**

Palīgrīki

- Notion - viskautkas
- Todoist - kas jādara?
- Toggl - laiks

Mīļākie resursi

- Tviteris (X) - jā, tiešām...
- Hackerone, pentest.land
- **Google**
- Random atradumi, kas man ir GitHub favorītos

Laužņi

- Burp suite, caido
- ffuf
- nmap
- dev tools
- Jeb kas, kas der situācijai

Tūlīt būs viss...

Kur mani atrast?

- Adresi neteikšu pagaidām
- Urķu platformas:
  - https://app.hackthebox.com/users/544386
  - https://tryhackme.com/p/cny
- Sociālie:
  - https://www.linkedin.com/in/gvido-b%C4%93rzi%C5%86%C5%A1/
  - https://www.instagram.com/gvidonis/
  - https://x.com/Cny33988539
- Izstrāde
  - https://github.com/gvido-berzins
  - https://github.com/cnyllou - kiberdrošības tematika

Jautājumi?

Droši jautājat jebko