

Mi az a Bug Bounty és hogyan kezdhetünk bele?

David Schütz - @xdavidhu

whoami

*bocsánat, magyarul ez valami
elképesztően furcsa*

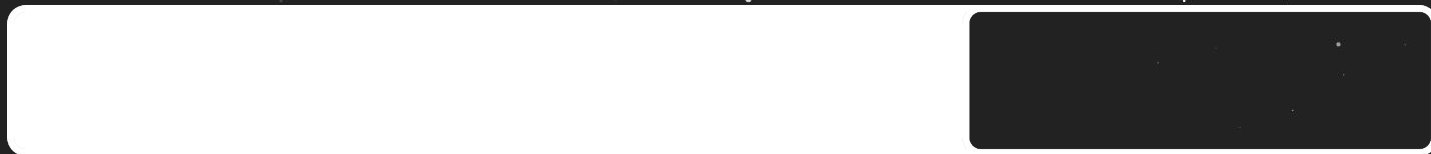
- I am...
 - bug hunter, web developer / maker / éppen ami
 - középiskolás
 - 2018 as Bugcrowd MVP, azért van rajtam a póló is mert sehol máshol nem értékelnék az emberek
 - InsecureSpace nevű podcast co-hostja, Spacehuhn-al



@xdavidhu

az előadás

15p



10p
Prezentáció

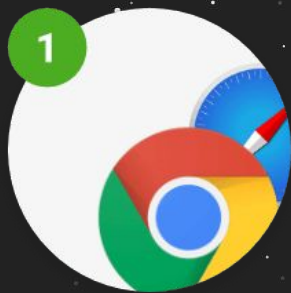


5p
Kérdések



@xdavidhu

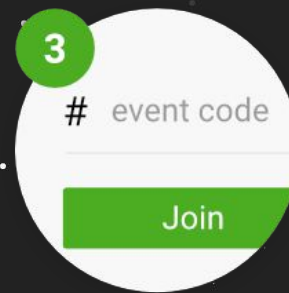
sli.do



nyisd meg a
böngészőt



menj a
<https://sli.do>-ra



írd be az event
code-ot

#hwswwb



1. rész

hogyan jutottunk el idáig?



az első “bug bounty” program

1983
Hunter & Ready



Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway. There's a catch, though. Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing. And since it's delivered in 4K bytes of ROM, VRTX will perform for

you the way it's performing in hundreds of real-time applications from avionics to video games. Bug free.

So, to save up to 12 months of development time, and maybe get a loveable little car from the junk yard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—28000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system

calls and interrupts. And when you call our system's error-reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER & READY
VRTX
Operating Systems in Silicon.

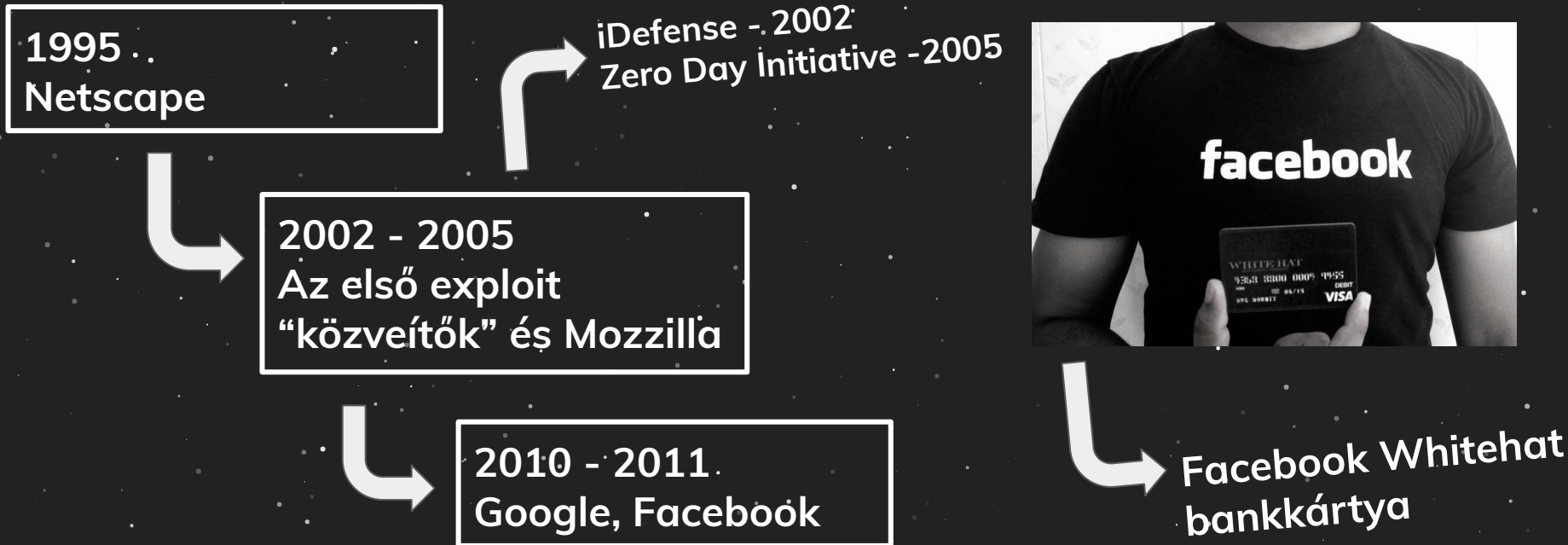
*Call or write for details. But, considering our taste in cars, you might want to accept our offer of \$1,000 cash instead. © 1983 Hunter & Ready, Inc.

But don't feel bad if in a year from now there isn't a bug in your driveway.
There isn't one in your operating system either.



@xdavidhu

őket követték...



és a mai platformok:



Bugcrowd
2011



HackerOne
2012



Synack
2013

és még sokan mások...



hogyan működnek?



Hackerek

Közvetítő platform

Cég



2. rész

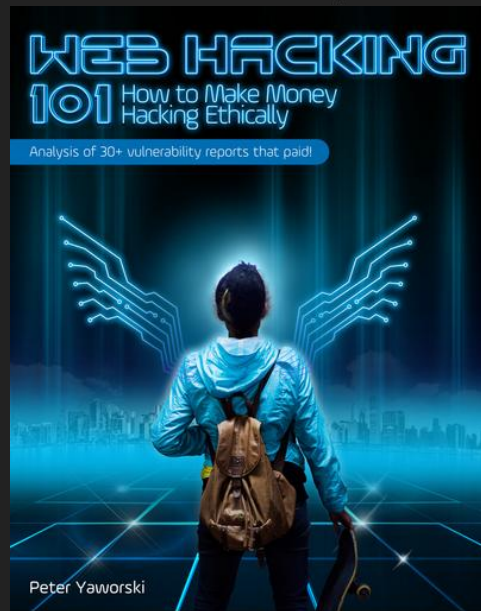
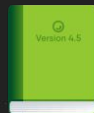
hogyan kezdhetünk bele?



@xdavidhu

1. lépés - tanulás

- alapok megértése, folyamatos tanulás
 - könyvek / olvasnivalók:
 - OWASP Top 10
 - Web Hacking 101 - Peter Yaworski
 - HackerOne reportok / Writeup-ok / Blog-ok
 - előadások / videók:
 - The Bug Hunters Methodology - Jason Haddix
 - LevelUp - Bugcrowd
 - Hacker101 - HackerOne
 - bug hunter közösség & Twitter
 - sok más bug hunter követése -> bug bounty
 - Twitter feed -> új infók / közösség
- + még sok más

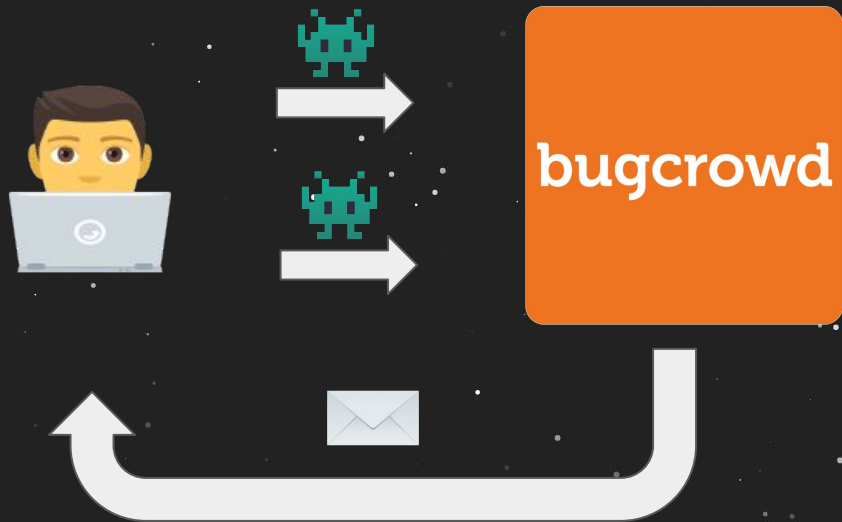


@xdavidhu

2. lépés - első bugok

- első program:
 - kudos/point only
 - rendes, fizető program
- pár elfogadott bug -> privát program meghívók
- privát programok előnyei:
 - kevesebb ember
 - eddig nem tesztelt, új felületek
 - nagyobb esély / könnyebb bugokat találni

vita



privát programok

(de! nem feltétlen
kell privát program)



@xdavidhu

3. lépés - kitartás / gondolatmenet

- lehet hogy sokszor órákig nem fogsz találni semmit
 - de! ez nem jelenti azt hogy rosszul csinálod
- lehet hogy ha találsz valamit amit már valaki korábban bejelentett és duplicate lesz
- lehet hogy lesznek olyan dolgok amit igazságtalannak tártsz
 - sajnos a cégek / platformok döntenek mindenről, minél több bugot találsz, annál több lesz elfogadva



NEM stabil bevétel!



@xdavidhu

3. lépés - kitartás / gondolatmenet

“ezt már úgyis annyian megnézték”

“tuti nem lehet már benne semmit
sem találni”

“annyi ideje megy már hogy biztos
hogy nincs...”

“publikus programokat már rengetegen
letesztelték”



ha ezeket le tudod
magadban “győzni”, már
rengeteg ember előtt vagy



miért különleges?

- ha találtál egy bugot nem számít hogy ki / hány éves / hol vagy és hogy milyen papírod van, az akkor is ott lesz!
- óriási cégekkel dolgozhatsz együtt akik csak miattad fognak változtatni / fogják kijavítani a termékeiket!
- a pénzen kívül, elmondhatod hogy “meghackeltél” egy ilyen méretű céget!



a tudásod alapján
fognak megítélni, és
nem bármi más miatt!



“To earn more, you
must learn more!”

Brian Tracy



@xdavidhu

és a végére...
kérdések?

(remélhetőleg lesznek)



@xdavidhu

köszönöm a figyelmet!

youtube csatornám:

youtube.com/c/xdavidhu

podcastunk:

insecurespace.com

twitter/minden más:

[@xdavidhu](https://twitter.com/xdavidhu)



[@xdavidhu](https://twitter.com/xdavidhu)