

The Unreasonable Effectiveness of Audit Contests


DeFi Security Summit

August 28, 2022












SHERLOCK


What is an Audit Contest?

 **code4rena**

Contest ran 19 January 2022–26 January 2022

7 day contest


#	COMPETITOR	USD	TOTAL
1	 GregArt	\$11,521.89	18
2	 OviCabush	\$11,273.85	6
3	 egilmm1	\$10,957.14	1
4	 kirk_baer	\$7,330.80	2
5	 Basilix	\$7,049.05	9
6	 huh	\$3,303.57	6
7	 static	\$3,287.14	1
8	 airhatchel	\$3,128.52	5
9	 ye0ide	\$2,494.83	4



Sherlock contest
Decentralized exploit protection.

[VIEW REPO](#) [VIEW REPORT](#)

\$80,000 USDC
TOTAL AWARDS



Audit Contest Data

[Public] C4 Exploit Data																										
File Edit View Insert Format Data Tools Extensions Help Last edit was made 2 minutes ago by Jack Stanford																										
100% 1000 123+ Default (tab...) 10																										
A1																										
	id	title	end_time_for_reward	end_time_reward	time_since_today	amount	repo	findingsRepo	hide	language	Protocol	count	Hacked	Hack Date	Hack writeup	Relevant to C4 audit?	Caught by C4	C4 report	If caught, where	Need confirmation?	Cause	Bug Bounty / Exploit Fix	Mon			
1	1	1	2021-03-27	2021-03-27	0	551 \$20,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
2	2	2	2021-03-03	2021-03-03	0	542 22 ETH	https://github.com/https://github.com	FALSE	eth	1	0															
3	3	3	2021-04-07	2021-04-07	0	307 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
4	4	4	2021-04-21	2021-04-21	0	493 \$100,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
5	5	5	2021-04-28	2021-04-28	0	486 27 ETH + 1000	https://github.com/https://github.com	FALSE	eth	1	0															
6	6	6	2021-05-07	2021-05-07	0	483 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	1/5/20	https://github.com/https://github.com													
7	7	7	2021-05-04	2021-05-04	0	480 \$30,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
8	8	8	2021-05-11	2021-05-11	0	473 \$60,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
9	9	9	2021-05-19	2021-05-19	0	465 \$45,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	1/1/17	https://github.com/https://github.com													
10	10	10	2021-05-19	2021-05-19	0	465 \$60,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	1/2/17	https://github.com/https://github.com													
11	11	11	2021-05-20	2021-05-20	0	458 \$55,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
12	12	12	2021-06-02	2021-06-02	0	451 \$100,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	2/27/20	https://github.com/https://github.com													
13	13	13	2021-06-16	2021-06-16	0	437 \$45,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
14	14	14	2021-06-27	2021-06-27	0	430 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
15	15	15	2021-06-30	2021-06-30	0	423 \$100,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
16	16	16	2021-07-07	2021-07-07	0	416 \$100,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
17	17	17	2021-07-14	2021-07-14	0	409 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	5/27/20	https://github.com/https://github.com													
18	18	18	2021-07-11	2021-07-11	0	412 \$25,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
19	19	19	2021-07-01	2021-07-01	0	402 \$80,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	5/20/20	https://github.com/https://github.com													
20	20	20	2021-07-28	2021-07-28	0	395 \$80,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
21	21	21	2021-07-28	2021-07-28	0	391 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
22	22	22	2021-09-08	2021-09-08	0	381 \$100K USD +	https://github.com/https://github.com	FALSE	eth	1	0															
23	23	23	2021-07-31	2021-07-31	0	382 \$20,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
24	24	24	2021-08-14	2021-08-14	0	376 \$30,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
25	25	25	2021-08-25	2021-08-25	0	367 \$30,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
26	26	26	2021-09-08	2021-09-08	0	353 \$100,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
27	27	27	2021-09-10	2021-09-10	0	346 \$100,000 (0.00)	https://github.com/https://github.com	FALSE	eth	1	1	9/17/20	https://github.com/https://github.com													
28	28	28	2021-09-29	2021-09-29	0	332 \$200,000 (0.00)	https://github.com/https://github.com	FALSE	eth	0	dupes															
29	29	29	2021-09-29	2021-09-29	0	326 \$30,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
30	30	30	2021-09-08	2021-09-08	0	353 \$30,000 USD	https://github.com/https://github.com	FALSE	eth	1	1	1/2/20	https://github.com/https://github.com													
31	31	31	2021-09-29	2021-09-29	0	323 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
32	32	32	2021-10-08	2021-10-08	0	325 \$100,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
33	33	33	2021-10-13	2021-10-13	0	318 \$105,000 USD	https://github.com/https://github.com	FALSE	eth	0	dupes															
34	34	34	2021-10-08	2021-10-08	0	325 \$100,000 (0.00)	https://github.com/https://github.com	FALSE	eth	0	dupes															
35	35	35	2021-09-27	2021-09-27	0	339 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
36	36	36	2021-10-27	2021-10-27	0	311 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
37	37	37	2021-10-27	2021-10-27	0	313 \$50,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
38	38	38	2021-10-08	2021-10-08	0	325 \$75,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															
39	39	39	2021-10-13	2021-10-13	0	318 \$30,000 USD	https://github.com/https://github.com	FALSE	eth	1	0															

https://docs.google.com/spreadsheets/d/1RIJCK3_9RHvtNPObsDRTAqkP9lbyutZMsqlKNnZCO00/edit?usp=sharing

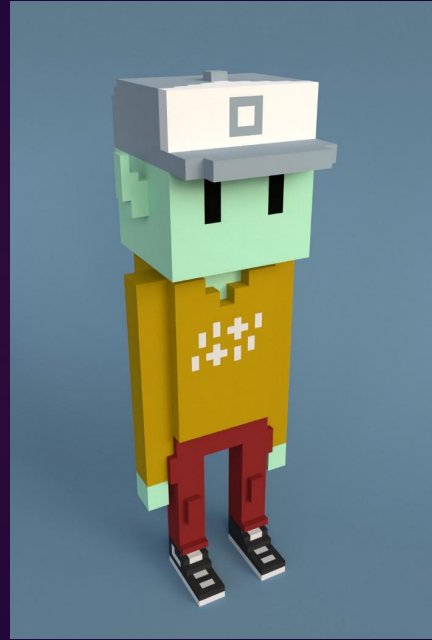
Audit Contest Data

- 1.5 years since first contest
- 154 unique contests
- 110 unique protocols
- Average contest finished 7.5 months ago

How many hacks?

Meebits

- Contest #7
- Ended May 1st, 2021
- Hacked May 8th, 2021
- Brute-forced rare Meebits

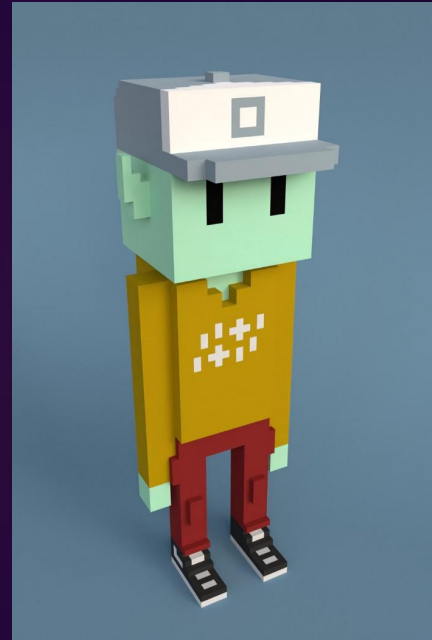


Meebits

- Contest #7
- Ended May 1st, 2021
- Hacked May 8th, 2021
- Brute-forced rare Meebits

[M-01]_RANDOMINDEX_IS NOT TRULY RANDOM - POSSIBILITY OF PREDICTABLY MINTING A SPECIFIC TOKEN ID

- Not fixed



Visor



- **Contest #9**
- **Ended May 19th, 2021**
- **Hacked June 19th, Nov 26th, Dec 21st, 2021**
 - **June 19th: Admin key stolen**
 - **Nov 26th: deposit() used spot price of a DEX**
 - **Dec 21st: deposit() asked attack contract to approve itself**

Visor



- **Contest #9**
- **Ended May 19th, 2021**
- **Hacked June 19th, Nov 26th, Dec 21st, 2021**
 - **June 19th: Admin key stolen**
 - **Nov 26th: deposit() used spot price of a DEX**
 - **Dec 21st: deposit() asked attack contract to approve itself**
- **All out of scope**

Days Since Last Incident:

∞

154 audits!!!

Problems with Audit Contests

- **No guarantee of top-tier auditors**
- **No guarantee of time spent on codebase**
- **No fix reviews**
- **Protocol team sorts through hundreds of issues**

Problems with Legacy Audits

- Only 2-3 people look at codebase
 - Example: High severity bug found by auditor #30 and #66
 - Missed by top-tier audit firm
- No direct incentive to secure codebase (only reputation)
- Often long lead times

Best of Both Worlds?

- **Dedicated, incentivized top-tier auditor**
- **Contest pot allowing anyone to compete and submit bugs**
- **Fix review**
- **Concisely reported issues**
- **On-demand scheduling**

Sherlock Next Generation Audits

- **\$75k cost to protocol (assuming 2-week audit)**
- **\$50k contest pot**
- **Top-tier auditor earns \$20k + pool earnings**
- **Top-tier auditor reviews fixes**
- **ELO-style rankings determine top-tier auditors**
- **Access to \$10M TVL coverage and \$1M bug bounty coverage**

Get Involved

- Sentiment contest launches tomorrow (Aug 29th)
- Security experts/teams of any level can join
- Sign up at sherlock.xyz



SHERLOCK