

Flash Loan and Re-entry Attack: Analysis of Grim Finance's Hacked Event



Dec 20th, 2021

On January 19, time on January 19, Fantom Finance suffered a lightning attack and lost more than 30 million US dollars. Grim Finance has all the vaults and reminded users to stop withdrawing their personal assets in time.

SharkTeam conducted an analysis and technical analysis of this incident, and concluded a security measure. It is hoped that chain projects in the chain industry can learn from this and build a blockchain security defense line.

1.Event analysis

During the entire attack process, the attackers attacked multiple LP vault contracts and single-currency vault contracts of Grim Finance, including the following transactions:

①	0xb5e99eff2a3f37bf3da9...	Start	25350117	2021-12-18 18:55:25	Grim Finance Exploiter 1	攻击WFTM单币金库, 获得 728019 WFTM OUT	0x360b65da2930ab6ffc8...	0 FTM
②	0xce6a505a6da960a8ce4...	Start	25350030	2021-12-18 18:52:55	Grim Finance Exploiter 1	攻击WFTM单币金库, 获得 15454993 WFTM OUT	0x360b65da2930ab6ffc8...	0 FTM
③	0x4b4c3b1cf0d2691a400...	0x60806040	25349987	2021-12-18 18:52:17	Grim Finance Exploiter 1	创建攻击WFTM单币金库的合约0x360b OUT Contract Creation		0 FTM
④	0x1e71556800bf072613...	Start	25349516	2021-12-18 18:45:32	Grim Finance Exploiter 1	攻击SpookyToken(BOO)单币金库, 获得 32412 BOO OUT	0xfecd91fe44868d795fdd...	0 FTM
⑤	0x753551a7d988346210...	Start	25349396	2021-12-18 18:43:56	Grim Finance Exploiter 1	攻击SpookyToken(BOO)单币金库, 获得 104238 BOO OUT	0xfecd91fe44868d795fdd...	0 FTM
⑥	0xa9593b408b5b91e962...	0x60806040	25349364	2021-12-18 18:43:30	Grim Finance Exploiter 1	创建攻击SpookyToken(BOO)单币金库的合约0xfecd OUT Contract Creation		0 FTM
⑦	0x03302ca39fd331830aa...	Any Swap Out Und...	25347440	2021-12-18 18:16:10	Grim Finance Exploiter 1	USDC跨链转账 OUT	Anyswap: Router v4	0 FTM
⑧	0x034bf9666b5db529eb7...	Approve	25347277	2021-12-18 18:13:23	Grim Finance Exploiter 1	OUT	Centre: USD Coin	0 FTM
⑨	0x584a3dd2bca7c5dc30...	Any Swap Out Und...	25347206	2021-12-18 18:12:08	Grim Finance Exploiter 1	DAI跨链转账 OUT	Anyswap: Router v4	0 FTM
⑩	0x1d66745c23b144593e...	Approve	25347123	2021-12-18 18:10:50	Grim Finance Exploiter 1	OUT	Maker: Dai Stablecoin	0 FTM

⑦	0x7b9ea370949331aadb...	Start	25347013	2021-12-18 18:09:00	Grim Finance Exploiter 1	攻击WFTM单币金库, 获得 170250 WFTM	OUT	0x577edc8d679ca0da67...	0 FTM
⑧	0xf14ca312081996d84c5...	Start	25346896	2021-12-18 18:05:04	Grim Finance Exploiter 1	攻击WFTM单币金库, 获得 1951895 WFTM	OUT	0x577edc8d679ca0da67...	0 FTM
⑨	0xc931dda5ccd4c92a954...	0x60806040	25346882	2021-12-18 18:04:48	Grim Finance Exploiter 1	创建攻击WFTM单币金库的合约0x577e	OUT	Contract Creation	0 FTM
⑩	0xa5413918bf6ab875726...	Start	25346190	2021-12-18 17:55:29	Grim Finance Exploiter 1	攻击BTC单币金库, 获得 14.67 BTC	OUT	0x1f8d2e68da1e4403586...	0 FTM
⑪	0xd3995539f275df9dff68...	0x60806040	25346175	2021-12-18 17:55:18	Grim Finance Exploiter 1	创建攻击BTC单币金库的合约0x1f8d	OUT	Contract Creation	0 FTM
⑫	0x497e6d97cb7ae75b33...	Start	25345012	2021-12-18 17:39:25	Grim Finance Exploiter 1	攻击DAI/USDC LP金库, 获得 755621 DAI + 755107 USDC	OUT	0x059c989a18990572a0...	0 FTM
⑬	0x19315e5b150d0a83e7...	Start	25345003	2021-12-18 17:39:15	Grim Finance Exploiter 1	攻击WFTM/BTC LP金库, 获得 11.78 BTC + 362770 WFTM	OUT	AttackerContract 0xb08c	0 FTM
⑭	0x18324bd873e10b02c9...	0x60806040	25344984	2021-12-18 17:38:56	Grim Finance Exploiter 1	创建攻击DAI/USDC LP金库的合约0x059c	OUT	Contract Creation	0 FTM
⑮	0x56b95c78d1d9405ba...	0x60806040	25344919	2021-12-18 17:38:03	Grim Finance Exploiter 1	创建攻击WFTM/BTC LP金库的合约0xb08c	OUT	Contract Creation	0 FTM
⑯	0x98ca417d299ce92c3c0...	0x60806040	25344743	2021-12-18 17:35:38	Grim Finance Exploiter 1	创建攻击合约0xd47c	OUT	Contract Creation	0 FTM

Finally, the obtained token will be transferred to other public chains through AnySwap cross-chain transfer. For example, the FTM cross-chain transaction is as follows:

⑦	0x2be615665c48237911...	Any Swap Out Nat...	25351014	2021-12-18 19:16:40	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑧	0x248112dede955b5777...	Any Swap Out Nat...	25350976	2021-12-18 19:15:42	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑨	0xb0418c27d1bebdcc66...	Any Swap Out Nat...	25350931	2021-12-18 19:14:43	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑩	0x4f20df36277ac2ba0d3...	Any Swap Out Nat...	25350904	2021-12-18 19:14:00	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑪	0x6d5ae6ded3572e4021...	Any Swap Out Nat...	25350852	2021-12-18 19:12:52	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑫	0x5a89593a01362246f66...	Any Swap Out Nat...	25350766	2021-12-18 19:10:28	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑬	0x08d4291cebb1675460...	Any Swap Out Nat...	25350705	2021-12-18 19:09:08	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑭	0x9da050651094c7761b...	Any Swap Out Nat...	25350665	2021-12-18 19:08:12	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑮	0x7dd2683d282c4c8be6...	Any Swap Out Nat...	25350521	2021-12-18 19:04:35	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑯	0x4f645f795ce4c6684da...	Any Swap Out Nat...	25350440	2021-12-18 19:02:26	Grim Finance Exploiter 1	OUT	0xf3ce95ec61114a4b1bf...	400,000 FTM
⑰	0xae02398f7d4de070484...	Withdraw	25350347	2021-12-18 19:00:38	Grim Finance Exploiter 1	OUT	WFTM 将WFTM转换成FTM	0 FTM

Taking transaction

0x19315e5b150d0a83e797203bb9c957ec1fa8a6f404f4f761d970cb29a74a5dd6 as an example, the detailed description of the attack project is as follows:

1. Flash loans and add liquidity. Borrow 937830 WFTM and 30 BTC through a flash loan, then add liquidity to the WFTM/BTC Pancake trading pair to get 0.0476 SPIRIT-LP liquidity certificate.

From Vault	To AttackerContract	For 937,830 (\$1,331,718.60)	Wrapped Fant... (WFTM)	闪电贷
From Vault	To AttackerContract	For 30 (\$1,399,680.00)	Bitcoin (BTC)	
From AttackerContract	To WFTM/BTC-SPIRIT...	For 30 (\$1,399,680.00)	Bitcoin (BTC)	添加流动性
From AttackerContract	To WFTM/BTC-SPIRIT...	For 923,575.591715867110610192 (\$1,311,477.34)	Wrapped Fant... (WFTM)	
From Null Address: 0x00...	To SpiritMaker	For 0.000000030478124368	Spirit LPs (SPIRIT...)	生成流动性凭证
From Null Address: 0x00...	To AttackerContract	For 0.047610132146053993	Spirit LPs (SPIRIT...)	

2. Pledge liquidity vouchers to the vault contract and mint share tokens.

From AttackerContract	To GrimBoostVault-BT...	For 0.047610132146053993	Spirit LPs (SPIRIT...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0.047610132146053993	Spirit LPs (SPIRIT...)
From GrimBoostStrategy	To 0x928144cd396ac...	For 0.047610132146053993	Spirit LPs (SPIRIT...)
From 0x928144cd396ac...	To Gauge	For 0.047610132146053993	Spirit LPs (SPIRIT...)
From Gauge	To SpiritMaker	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 0.032376253762624097	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 0.11472715832368394	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 0.406542429322769007	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 1.440606995366844921	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 5.10487556872493898	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 18.089426648611236895	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 64.100946647994200627	GB-BTC-FTM (GB-BTC...)
From GrimBoostVault-BT...	To GrimBoostStrategy	For 0	Spirit LPs (SPIRIT...)
From Null Address: 0x00...	To AttackerContract	For 227.145472379272462836	GB-BTC-FTM (GB-BTC...)

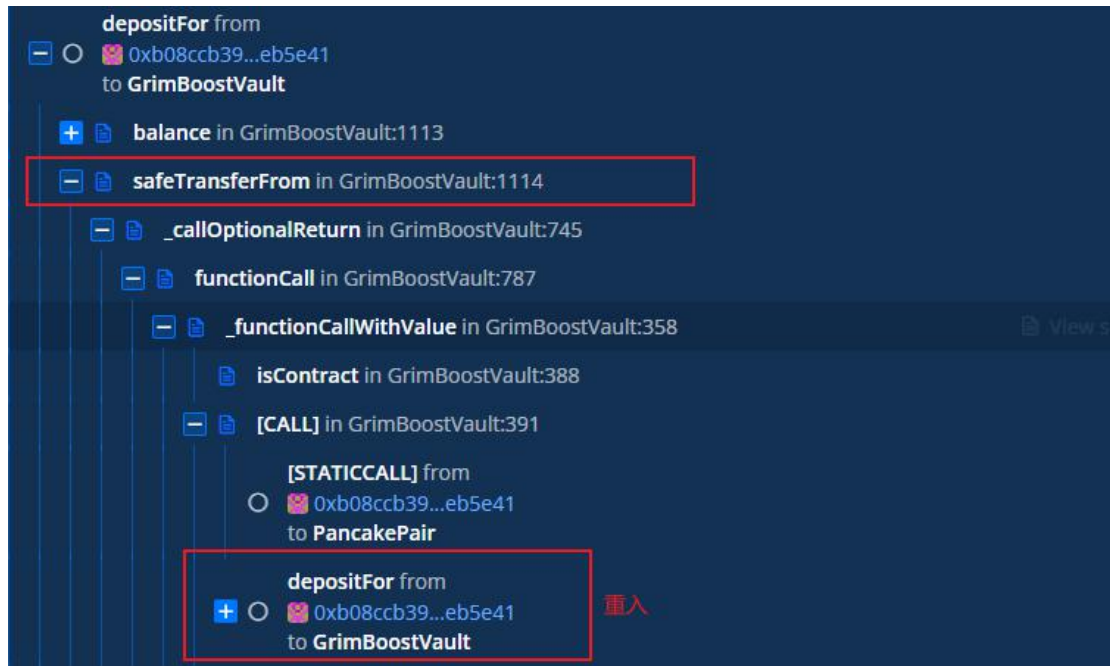
The attack contract pledged the liquidity token to the vault through the depositFor function in the GrimBoostVault contract, and minted 316 GB-BTC-FTM share tokens.

```
1115 function depositFor(address token, uint _amount, address user ) public {
1116
1117     uint256 pool = balance();
1118     IERC20(token).safeTransferFrom(msg.sender, address(this), _amount);
1119     earn();
1120     uint256 _after = balance();
1121     _amount = _after.sub(pool); // Additional check for deflationary tokens
1122     uint256 shares = 0;
1123     if (totalSupply() == 0) {
1124         shares = _amount;
1125     } else {
1126         shares = (_amount.mul(totalSupply())).div(pool);
1127     }
1128     _mint(user, shares);
1129 }
```

In this process, because the depositFor function does not verify the parameter token, that is, any token can be passed to mint share tokens, and the attacker contract can mint share tokens by passing a custom token contract (attack contract address).

```
{
  "[FUNCTION]" : "depositFor",
  "[OPCODE]" : "CALL",
  "from" : {
    "address" : "0xb08ccb39741d746dd1818641900f182448eb5e41",
    "balance" : "0"
  },
  "to" : {
    "address" : "0x660184ce8af80e0b1e5a1172a16168b15f4136bf",
    "balance" : "0"
  },
  "value" : "0",
  "input" : {
    自定义Token, 攻击合约
    "token" : "0xb08ccb39741d746dd1818641900f182448eb5e41",
    "_amount" : "47610132146053993",
    "user" : "0xb08ccb39741d746dd1818641900f182448eb5e41"
  },
  "[OUTPUT]" : "0x",
  "gas" : {
    "gas_left" : 1395366,
    "gas_used" : 967233,
    "total_gas_used" : 460578
  }
}
```

The reentrancy of the depositFor function is implemented multiple times through the safeTransferFrom function in the custom token contract.



Pass the correct WFTM/BTC SPIRIT-LP transaction pair address and 0.0476 SPIRIT-LP in the last reentrant call to the `depositFor` function.

```

{
  "[FUNCTION]" : "depositFor"
  "[OPCODE]" : "CALL"
  "from" : {
    "address" : "0xb08ccb39741d746dd1818641900f182448eb5e41"
    "balance" : "0"
  }
  "to" : {
    "address" : "0x660184ce8af80e0b1e5a1172a16168b15f4136bf"
    "balance" : "0"
  }
  "value" : "0"
  "input" : {
    "token" : "0x279b2c897737a50405ed2091694f225d83f2d3ba"
    "_amount" : "47610132146053993"
    "user" : "0xb08ccb39741d746dd1818641900f182448eb5e41"
  }
  "[OUTPUT]" : "0x"
  "gas" : {
    "gas_left" : 916120
    "gas_used" : 340417
    "total_gas_used" : 939824
  }
}

```

WFTM/BTC SPIRIT-LP

This repeated minting of share tokens eventually allowed the GrimBoostVault contract to mint far more share tokens (316 GB-BTC-FTM) for the attacker than expected.

3. Withdraw liquidity certificates based on share tokens.

From AttackerContract	To Null Address: 0x00...	For 316.434974081378761303	GB-BTC-FTM (GB-BTC...)
From Gauge	To 0x928144cd396ac...	For 0.06632538511043804	Spirit LPs (SPIRIT...)
From 0x928144cd396ac...	To GrimBoostStrategy	For 0.06632538511043804	Spirit LPs (SPIRIT...)
From GrimBoostStrategy	To GrimBoostVault-BT...	For 0.06632538511043804	Spirit LPs (SPIRIT...)
From GrimBoostVault-BT...	To AttackerContract	For 0.06632538511043804	Spirit LPs (SPIRIT...)

The attack contract has withdrawn 0.0663 SPIRIT-LP based on the minted far more tokens than expected (316 GB-BTC-FTM), which is significantly more than the actual pledged 0.0476 SPIRIT-LP.

4. Remove liquidity and repay the flash loan.

From AttackerContract	To WFTM/BTC-SPIRIT...	For 0.06632538511043804	Spirit LPs (SPIRIT...)	
From WFTM/BTC-SPIRIT...	To Null Address: 0x00...	For 0.06632538511043804	Spirit LPs (SPIRIT...)	移除流动性
From WFTM/BTC-SPIRIT...	To AttackerContract	For 1,286,627.531535482533090765 (\$1,827,011.09)	Wrapped Fant... (WFTM)	
From WFTM/BTC-SPIRIT...	To AttackerContract	For 41.79281727 (\$1,949,885.68)	Bitcoin (BTC)	
From AttackerContract	To Vault	For 938,111.349 (\$1,332,118.12)	Wrapped Fant... (WFTM)	
From AttackerContract	To Vault	For 30.009 (\$1,400,099.90)	Bitcoin (BTC)	
From Vault	To ProtocolFeesCollec...	For 281.349 (\$399.52)	Wrapped Fant... (WFTM)	
From Vault	To ProtocolFeesCollec...	For 0.009 (\$419.90)	Bitcoin (BTC)	闪电贷还款

5. Transfer the remaining 362,770 WFTM and 11.78 BTC to the attacker's account address.

From AttackerContract	To Grim Finance Explo...	For 11.78381727 (\$549,785.78)	Bitcoin (BTC)	
From AttackerContract	To Grim Finance Explo...	For 362,770.590819615422480573 (\$515,134.24)	Wrapped Fant... (WFTM)	

The root cause of this attack is: because the depositFor function in the Grim contract does not verify the parameter token, that is, any token can be passed to mint share tokens. The attacker mints share tokens by passing a custom token contract (attack contract address), and re-enters the depositFor function through the safeTransferFrom function in the custom token contract, which eventually causes the GrimBoostVault contract to mint far more than expected for the attacker of share tokens (316 GB-BTC-FTM).

2. safety recommendations

This incident is another security incident related to lightning loans. The business logic design of the DeFi project is complex, involving many economic calculations and parameters, but the composability between different projects and agreements is extremely rich and difficult to predict. Prone to security breaches. As shown in the table below, the number of DeFi incidents that used

flash loans to attack this new product has been endless in the past year, which has increased to 46. Generally, lightning loan attacks include four types:

"raising arbitrage," "oracles manipulation," "re-entry attacks," and "technical vulnerabilities." This is a lightning loan attack based on the use of "oracles".

编号	日期	主攻协议	闪电贷协议	攻击类型
1	2020/2/15	bZx	dYdX	哄抬套利
2	2020/2/18	bZx	bZx	操纵预言机
3	2020/6/28	Balancer	dYdX	哄抬套利
4	2020/10/26	Harvest	Uniswap V2	操纵预言机
5	2020/11/6	Cheese Bank	dYdX	操纵预言机
6	2020/11/12	Akropolis	dYdX	重入攻击
7	2020/11/14	Value.DeFi	Aave/Uniswap V2	操纵预言机
8	2020/11/17	OUSD	dYdX	重入攻击
9	2020/12/18	Warp Finance	Uniswap V2/dYdX	操纵预言机
10	2021/2/4	Yearn.Finance	dYdX/Aave	哄抬套利
11	2021/2/13	Alpha.Finance	Aave	技术漏洞
12	2021/5/2	Spartan	PancakeSwap	哄抬套利
13	2021/5/8	Value.DeFi	Value.DeFi	技术漏洞
14	2021/5/8	Rari Capital	dYdX	重入攻击
15	2021/5/13	xToken	dYdX	操纵预言机
16	2021/5/16	bEarn Fi	Cream.Finance	技术漏洞
17	2021/5/20	PancakeBunny	PancakeSwap	操纵预言机
18	2021/5/22	Bogged Finance	PancakeSwap	技术漏洞
19	2021/5/25	AutoShark	PancakeSwap	技术漏洞+操纵预言机
20	2021/5/28	BurgerSwap	PancakeSwap	重入攻击
21	2021/5/28	JulSwap	JulSwap	操纵预言机
22	2021/5/30	Belt Finance	PancakeSwap	操纵预言机
23	2021/6/5	BurgerSwap	PancakeSwap	重入攻击
24	2021/6/10	EvoDeFi	PancakeSwap	技术漏洞
25	2021/6/19	Impossible Finance	PancakeSwap	技术漏洞
26	2021/6/23	Eleven Finance	ApeSwap	技术漏洞
27	2021/6/25	xWin Finance	PancakeSwap	操纵预言机
28	2021/7/2	XDXSwap	XDXSwap (Heco)	技术漏洞
29	2021/7/13	DeFiPie	PancakeSwap	重入攻击
30	2021/7/14	ApeRocket	PancakeSwap	技术漏洞
31	2021/7/14	ApeRocket	AAVE (Polygon)	技术漏洞
32	2021/7/16	Swamp.Finance	PancakeSwap	技术漏洞
33	2021/7/17	PancakeBunny	AAVE (Polygon)	技术漏洞
34	2021/7/18	Array.Finance	AAVE	技术漏洞
35	2021/8/4	Popsicle Finance	AAVE	技术漏洞
36	2021/8/4	Wault.Finance	PancakeSwap	技术漏洞
37	2021/8/17	XSURGE	PancakeSwap	重入攻击
38	2021/8/25	Dot.Finance	PancakeSwap	技术漏洞
39	2021/8/30	Cream Finance	Uniswap V2	重入攻击
40	2021/9/12	Zabu Finance	Pangolin	技术漏洞
41	2021/9/15	NowSwap	NowSwap	技术漏洞
42	2021/10/2	Twindex	Twindex	技术漏洞
43	2021/10/2	AutoShark	PancakeSwap	操纵预言机
44	2021/10/6	MY FARM PET	PancakeSwap	操纵预言机
45	2021/10/15	Indexed Finance	SushiSwap	技术漏洞
46	2021/10/20	Pankehunny	PancakeSwap	操纵预言机

SharkTeam reminds you to be vigilant when getting involved in blockchain projects, choose more stable, safer, and complete multiple rounds of auditing public chains and projects. You must not put your assets at risk and become hackers. Cash machine. As the project party, the security of smart contracts is vital to the safety of users' property! The blockchain project party should cooperate with a professional security audit company to conduct multiple rounds of audits to avoid status and calculation errors in the contract, and provide guarantees for the security of users' digital assets and the security of the project itself.

As a leading blockchain security service team, SharkTeam provides developers with smart contract audit services. The smart contract audit service consists of manual audit and automated audit to meet the needs of different customers. It exclusively implements nearly two hundred audit contents covering the four aspects of high-level language layer, virtual machine layer, blockchain layer, and business logic layer, fully guaranteeing smart contracts Safety.

SharkTeam

About

SharkTeam focus on smart contract security, composed of members with many years of practical experience in front-line cyber security and blockchain. We are proficient in the underlying principles of blockchain and smart contract, and has perfect capabilities in blockchain vulnerability mining and smart contract audit. We can provide comprehensive threat modeling, smart contract audit and emergency response services, SharkTeam has helped several well-known blockchain projects find and fix security vulnerabilities, and is committed to protecting the security of users' digital assets and privacy.

Security Vulnerability



Security Service

7*24h online



Automated audit

- Automated scanning
- Exclusive coverage
- High precision



Manual audit service

- VIP Security Audit Service
- VIP compliance audit service
- Emergency response and contract customization

Partner



Twitter: @sharkteamorg



Telegram: <https://t.me/sharkteamorg>



SharkTeam

In Math, We Trust !



<https://t.me/sharkteamorg>



<https://twitter.com/sharkteamorg>