知道创宇

密级 ★ | 项目组公开

智能合约审计报告

安全状态

安全

★ ★ ★ ★ ★

主测人： 知道创宇区块链安全研究团队

版本说明

修订内容	时间	修订者	版本号
编写文档	20210316	知道创宇区块链安全研究团队	V2.0

文档信息

文档名称	文档版本	报告编号	保密级别
YouSwap 智能合约审计报告	V1.0	a8b882477a824d8d907e72fbc940fbdf	项目组公开

声明

创宇仅就本报告出具前已经发生或存在的事实出具本报告，并就此承担相应责任。对于出具以后发生或存在的事实，创宇无法判断其智能合约安全状况，亦不对此承担责任。本报告所作的安全审计分析及其他内容，仅基于信息提供者截至本报告出具时向创宇提供的文件和资料。创宇假设:已提供资料不存在缺失、被篡改、删减或隐瞒的情形。如已提供资料信息缺失、被篡改、删减、隐瞒或反映的情况与实际情况不符的，创宇对由此而导致的损失和不利影响不承担任何责任。

目录

1. 综述

本次报告有效测试时间是从 2021 年 3 月 12 日开始到 2021 年 3 月 13 日结束，在此期间针对 **YouSwap 智能合约的 YouSwap (YOU)代币代码、IDO 募集合约代码**的安全性和规范性进行审计并以此作为报告统计依据。

本次智能合约安全审计的范围，不包含外部合约调用，不包含未来可能出现的新型攻击方式，不包含合约升级或篡改后的代码(随着项目方的发展，智能合约可能会增加新的 pool、新的功能模块，新的外部合约调用等)，不包含前端安全与服务器安全。

此次测试中，知道创宇工程师对智能合约的常见漏洞（见第三章节）进行了全面的分析，综合评定为**通过**。

本次智能合约安全审计结果： 通过

由于本次测试过程在非生产环境下进行，所有代码均为最新备份，测试过程均与相关接口人进行沟通，并在操作风险可控的情况下进行相关测试操作，以规避测试过程中的生产运营风险、代码安全风险。

本次审计的报告信息：

报告编号：a8b882477a824d8d907e72fbc940fbdf

报告查询地址链接: https://attest.im/attestation/searchResult?qurey=a8b882477a824d8d907e72fbc940fbdf

本次审计的目标信息：

条目	描述	
Token 名称	YouSwap	
合约地址	TokenYou	0x1d32916CFA6534D261AD53E2498AB95505bd2510
	IDO	0x59E6639bEf44164BA44Aa58771b94DF30BC023A6

代码类型	代币代码、募集协议代码、以太坊智能合约代码
代码语言	solidity

合约文件及哈希：

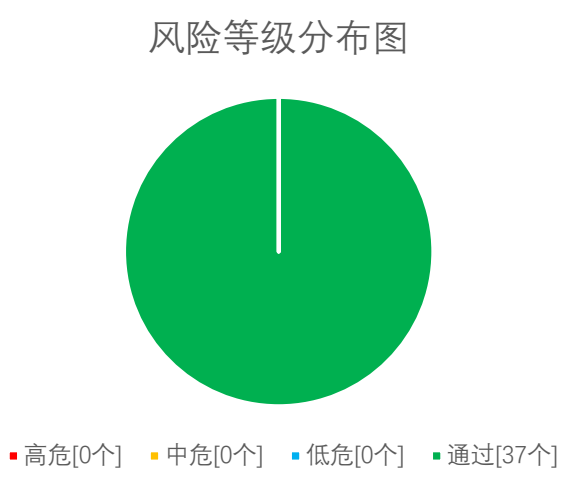
合约文件	MD5
TokenYou.sol	7d6a52a6d6fc88d388d3da123258fec1
IDO.sol	6e0de7c208535b77bb57e0ed967aef2f

2. 代码漏洞分析

2.1 漏洞等级分布

本次漏洞风险按等级统计：

安全风险等级个数统计表			
高危	中危	低危	通过
0	0	0	37



2.2 审计结果汇总说明

审计结果			
审计项目	审计内容	状态	描述
业务安全性检测	IDO 合约变量及构造函数	通过	经检测，不存在安全问题。
	IDO 合约白名单功能	通过	经检测，不存在安全问题。
	IDO 合约 privateOffering 函数	通过	经检测，不存在安全问题。
	IDO 合约 publicOffering 函数	通过	经检测，不存在安全问题。
	IDO 合约 withdrawPriIDO 函数	通过	经检测，不存在安全问题。
	IDO 合约 withdrawPubIDO 函数	通过	经检测，不存在安全问题。
	TokenYou 合约铸币功能	通过	经检测，不存在安全问题。
	TokenYou 合约销毁功能	通过	经检测，不存在安全问题。
	TokenYou 合约铸币权限管理功能	通过	经检测，不存在安全问题。
	TokenYou 合约基本代币功能	通过	经检测，不存在安全问题。
代码基本漏洞检测	编译器版本安全	通过	经检测，不存在该安全问题。
	冗余代码	通过	经检测，不存在该安全问题。
	安全算数库的使用	通过	经检测，不存在该安全问题。
	不推荐的编码方式	通过	经检测，不存在该安全问题。
	require/assert 的合理使用	通过	经检测，不存在该安全问题。
	fallback 函数安全	通过	经检测，不存在该安全问题。

	tx.orgin 身份验证	通过	经检测，不存在该安全问题。
	owner 权限控制	通过	经检测，不存在该安全问题。
	gas 消耗检测	通过	经检测，不存在该安全问题。
	call 注入攻击	通过	经检测，不存在该安全问题。
	低级函数安全	通过	经检测，不存在该安全问题。
	增发代币漏洞	通过	经检测，不存在该安全问题。
	访问控制缺陷检测	通过	经检测，不存在该安全问题。
	数值溢出检测	通过	经检测，不存在该安全问题。
	算数精度误差	通过	经检测，不存在该安全问题。
	错误使用随机数检测	通过	经检测，不存在该安全问题。
	不安全的接口使用	通过	经检测，不存在该安全问题。
	变量覆盖	通过	经检测，不存在该安全问题。
	未初始化的存储指针	通过	经检测，不存在该安全问题。
	返回值调用验证	通过	经检测，不存在该安全问题。
	交易顺序依赖检测	通过	经检测，不存在该安全问题。
	时间戳依赖攻击	通过	经检测，不存在该安全问题。
	拒绝服务攻击检测	通过	经检测，不存在该安全问题。
	假充值漏洞检测	通过	经检测，不存在该安全问题。
	重入攻击检测	通过	经检测，不存在该安全问题。
	重放攻击检测	通过	经检测，不存在该安全问题。
	重排攻击检测	通过	经检测，不存在该安全问题。

3. 业务安全性检测

3.1. IDO 合约变量及构造函数【通过】

审计分析：IDO 合约变量定义及构造函数设计合理。

```
contract IDO is Ownable {
    using SafeMath for uint256;

    //Private offering
    mapping(address => uint256) private _ordersOfPriIDO; //knownsec// 存储白名单用户的私募代币数量
    uint256 public startHeightOfPriIDO; //knownsec// 存储私募开始区块号
    uint256 public endHeightOfPriIDO; //knownsec// 存储私募结束区块号
    uint256 public totalUsdtAmountOfPriIDO = 0; //knownsec// 私募 USDT 总量
    uint256 public constant supplyYouForPriIDO = 5 * 10 ** 11;//50 万 YOU  //knownsec// 私募 You 代币供给量
    uint256 public reservedYouOfPriIDO = 0; //knownsec// 私募已发放 You 代币数量
    uint256 public constant upperLimitUsdtOfPriIDO = 500 * 10 ** 6;//500USDT //knownsec// 用户私募上限
    bool private _priOfferingFinished = false; //knownsec// 私募完成标识
    bool private _priIDOWithdrawFinished = false; //knownsec// 提现私募总量完成标识
    //knownsec// 私募相关事件
    event PrivateOffering(address indexed participant, uint256 amountOfYou, uint256 amountOfUsdt);
    event PrivateOfferingClaimed(address indexed participant, uint256 amountOfYou);

    //Public offering
    mapping(address => uint256) private _ordersOfPubIDO; //knownsec// 存储超募用户的超募 USDT 数量
    uint256 public constant targetUsdtAmountOfPubIDO = 5 * 10 ** 10;//5 万 USDT //knownsec// 超募目标 USDT 数量
    uint256 public constant targetYouAmountOfPubIDO = 5 * 10 ** 11;//50 万 YOU //knownsec//
```

```
超募目标 You 发放数量
    uint256 public totalUsdtAmountOfPubIDO = 0; //knownsec// 超募 USDT 总量
    uint256 public startHeightOfPubIDO; //knownsec// 超募开始区块号
    uint256 public endHeightOfPubIDO; //knownsec// 超募结束区块号
    uint256 public constant bottomLimitUsdtOfPubIDO = 100 * 10 ** 6; //100USDT //knownsec//
超募要求最少参与 USDT 数量
    bool private _pubIDOWithdrawFinished = false; //knownsec// 提现超募总量完成标识
    //knownsec// 超募相关事件
    event PublicOffering(address indexed participant, uint256 amountOfUsdt);
    event PublicOfferingClaimed(address indexed participant, uint256 amountOfYou);
    event PublicOfferingRefund(address indexed participant, uint256 amountOfUsdt);

    mapping(address => uint8) private _whiteList; //knownsec// 白名单列表

    address private constant _usdtToken = 0xdAC17F958D2ee523a2206206994597C13D831ec7;
    address private _youToken;

    uint256 public constant initialLiquidYou = 3 * 10 ** 12;//3 000 000YOU For initial Liquid
    address private constant _vault = 0x6B5C21a770dA1621BB28C9a2b6F282E5FC9154d5;

    uint private unlocked = 1;
    constructor(address youToken) public {
        _youToken = youToken;
    //knownsec// 初始化相关参数
        startHeightOfPriIDO = 12047150;
        endHeightOfPriIDO = 12048590;

        startHeightOfPubIDO = 0;
        endHeightOfPubIDO = 0;
    }
```

安全建议：无。

3.2. IDO 合约白名单功能【通过】

审计分析：IDO 合约的白名单功能按照合约业务需求正常限制调用者参与。

```
//knownsec// 白名单修饰器
modifier inWhiteList() {
    require(_whiteList[msg.sender] == 1, "YouSwap: NOT_IN_WHITE_LIST");
    _;
}

function isInWhiteList(address account) external view returns (bool) {
    return _whiteList[account] == 1;
}
//knownsec// 添加白名单
function addToWhiteList(address account) external onlyOwner {
    _whiteList[account] = 1;
}
//knownsec// 批量添加白名单
function addBatchToWhiteList(address[] calldata accounts) external onlyOwner {
    for (uint i = 0; i < accounts.length; i++) {
        _whiteList[accounts[i]] = 1;
    }
}
//knownsec// 移除白名单
function removeFromWhiteList(address account) external onlyOwner {
    _whiteList[account] = 0;
}
```

安全建议：无。

3.3. IDO 合约 privateOffering 函数【通过】

审计分析：IDO 合约的 privateOffering 函数用于参与私募，限制白名单用户

参与，其他普通用户不可参与私募。

```
    //knownsec// 参与私募
    function privateOffering(uint256 amountOfUsdt) inWhiteList external lock returns (bool) {
        //knownsec// 参与条件限制
        require(block.number >= startHeightOfPriIDO, 'YouSwap:NOT_STARTED_YET');
        require(!_priOfferingFinished && block.number <= endHeightOfPriIDO, 'YouSwap:PRIVATE_OFFERING_ALREADY_FINISHED');
        require(_ordersOfPriIDO[msg.sender] == 0, 'YouSwap: ENROLLED_ALREADY'); //knownsec// 仅可参与一次私募
        require(amountOfUsdt <= upperLimitUsdtOfPriIDO, 'YouSwap: EXCEEDS_THE_UPPER_LIMIT');
        require(amountOfUsdt > 0, "YouSwap: INVALID_AMOUNT");

        require(reservedYouOfPriIDO < supplyYouForPriIDO, 'YouSwap:INSUFFICIENT_YOU');
        uint256 amountOfYou = amountOfUsdt.mul(10);
        //0.1USDT/YOU
        //knownsec// 判断私募是否完成
        if (reservedYouOfPriIDO.add(amountOfYou) >= supplyYouForPriIDO) {
            amountOfYou = supplyYouForPriIDO.sub(reservedYouOfPriIDO);
            amountOfUsdt = amountOfYou.div(10);

            _priOfferingFinished = true;
        }
        _transferFrom(_usdtToken, amountOfUsdt); //knownsec// 提前授权本合约后将私募USDT 转入本合约地址

        _ordersOfPriIDO[msg.sender] = amountOfYou; //knownsec// 写入私募 You 代币数量记录
        reservedYouOfPriIDO = reservedYouOfPriIDO.add(amountOfYou); //knownsec// 累计发放 You 代币数量更新
        totalUsdtAmountOfPriIDO = totalUsdtAmountOfPriIDO.add(amountOfUsdt);
```

```
//knownsec// 私募参与总量更新
        emit PrivateOffering(msg.sender, amountOfYou, amountOfUsdt);

        return true;
    }
```

安全建议：无。

3.4. IDO 合约 publicOffering 函数【通过】

审计分析：IDO 合约的 publicOffering 函数用于参与超募，任何用户可参与超募。

```
    //knownsec// 参与超募
    function publicOffering(uint256 amountOfUsdt) external lock returns (bool)  {
        //knownsec// 参与条件限制
        require(block.number >= startHeightOfPubIDO, 'YouSwap:PUBLIC_OFFERING_NOT_STARTED_YET');
        require(block.number <= endHeightOfPubIDO, 'YouSwap:PUBLIC_OFFERING_ALREADY_FINISHED');
        require(amountOfUsdt >= bottomLimitUsdtOfPubIDO, 'YouSwap:100USDT_AT_LEAST');

        _transferFrom(_usdtToken, amountOfUsdt); //knownsec// 提前授权本合约后将超募USDT 转入本合约地址

        _ordersOfPubIDO[msg.sender] = _ordersOfPubIDO[msg.sender].add(amountOfUsdt); //knownsec// 更新用户超募数量
        totalUsdtAmountOfPubIDO = totalUsdtAmountOfPubIDO.add(amountOfUsdt); //knownsec// 更新超募总量

        emit PublicOffering(msg.sender, amountOfUsdt);
```

```
        _whiteList[msg.sender] = 1; //knownsec// 参与超募后自动成为白名单用户

        return true;
    }
```

安全建议：无。

3.5. IDO 合约 withdrawPriIDO 函数【通过】

审计分析：IDO 合约的 withdrawPriIDO 函数用于提取私募 USDT，仅 owner 可进行该操作。

```
    //knownsec// 提取私募 USDT
    function withdrawPriIDO() onlyOwner external {
        //knownsec// 提取限制
        require(block.number > endHeightOfPriIDO, 'YouSwap: BLOCK_HEIGHT_NOT_REACHED');
        require(!_priIDOWithdrawFinished, 'YouSwap: PRI_IDO_WITHDRAWN_ALREADY'); //knownsec// 仅可提取一次

        _transfer(_usdtToken, _vault, totalUsdtAmountOfPriIDO); //knownsec// 将合约内全部私募 USDT 转入指定地址
        _priIDOWithdrawFinished = true;
    }
```

安全建议：无。

3.6. IDO 合约 withdrawPubIDO 函数【通过】

审计分析：IDO 合约的 withdrawPubIDO 函数用于提取超募 USDT，仅 owner 可进行该操作。

```
    //knownsec// 提取超募 USDT
    function withdrawPubIDO() onlyOwner external {
```

```
        //knownsec// 提取限制
        require(block.number > endHeightOfPubIDO, 'YouSwap:
BLOCK_HEIGHT_NOT_REACHED');
        require(!_pubIDOWithdrawFinished, 'YouSwap:
PUB_IDO_WITHDRAWN_ALREADY'); //knownsec// 仅可提取一次

        uint256 amountToWithdraw = totalUsdtAmountOfPubIDO;
        //knownsec// 如参与量超过目标量，仅可提取目标超募数量
        if (totalUsdtAmountOfPubIDO > targetUsdtAmountOfPubIDO) {
            amountToWithdraw = targetUsdtAmountOfPubIDO;
        }

        _transfer(_usdtToken, _vault, amountToWithdraw); //knownsec// 将合约内全部超募
USDT 转入指定地址

        _mintYou(_youToken, _vault, initialLiquidYou); //knownsec// 提取结束后向_vault 地址
铸造指定数量的代币

        _pubIDOWithdrawFinished = true;
    }
```

安全建议：无。

3.7. TokenYou 合约铸币功能【通过】

审计分析：TokenYou 合约的铸币功能用于向指定地址铸造 You 代币，仅 minter 权限用户可进行该操作。

安全建议：无

3.8. TokenYou 合约销毁功能【通过】

审计分析：TokenYou 合约销毁功能用于销毁账户一定数量 You 代币。

安全建议：无。

3.9. TokenYou 合约铸币权限管理功能【通过】

审计分析：TokenYou 合约铸币权限用于管理铸币功能，仅 owner 可进行添加和移除 minter 操作。

安全建议：无。

3.10. TokenYou 合约基本代币功能【通过】

审计分析：TokenYou 合约基本功能符合 ERC20 代币基本功能。

```
/**
 *Submitted for verification at Etherscan.io on 2021-03-15
*/

//SPDX-License-Identifier: SimPL-2.0
pragma solidity ^0.6.0;

library SafeMath {
    /**
     * @dev Returns the addition of two unsigned integers, reverting on
     * overflow.
     *
     * Counterpart to Solidity's `+` operator.
     *
     * Requirements:
     *
     * - Addition cannot overflow.
     */
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
```

```
        uint256 c = a + b;
        require(c >= a, "SafeMath: addition overflow");

        return c;
    }

    /**
     * @dev Returns the subtraction of two unsigned integers, reverting on
     * overflow (when the result is negative).
     *
     * Counterpart to Solidity's `-` operator.
     *
     * Requirements:
     *
     * - Subtraction cannot overflow.
     */
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");
    }

    /**
     * @dev Returns the subtraction of two unsigned integers, reverting with custom message on
     * overflow (when the result is negative).
     *
     * Counterpart to Solidity's `-` operator.
     *
     * Requirements:
     *
     * - Subtraction cannot overflow.
     */
    function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        require(b <= a, errorMessage);
```

```
        uint256 c = a - b;

        return c;
    }

    /**
     * @dev Returns the multiplication of two unsigned integers, reverting on
     * overflow.
     *
     * Counterpart to Solidity's `*` operator.
     *
     * Requirements:
     *
     * - Multiplication cannot overflow.
     */
    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
        // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
        // benefit is lost if 'b' is also tested.
        // See: https://github.com/OpenZeppelin/openzeppelin-contracts/pull/522
        if (a == 0) {
            return 0;
        }

        uint256 c = a * b;
        require(c / a == b, "SafeMath: multiplication overflow");

        return c;
    }

    /**
     * @dev Returns the integer division of two unsigned integers. Reverts on
     * division by zero. The result is rounded towards zero.
     *
```

```
     * Counterpart to Solidity's `/` operator. Note: this function uses a
     * `revert` opcode (which leaves remaining gas untouched) while Solidity
     * uses an invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        return div(a, b, "SafeMath: division by zero");
    }

    /**
     * @dev Returns the integer division of two unsigned integers. Reverts with custom message
on
     * division by zero. The result is rounded towards zero.
     *
     * Counterpart to Solidity's `/` operator. Note: this function uses a
     * `revert` opcode (which leaves remaining gas untouched) while Solidity
     * uses an invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256)
{
        require(b > 0, errorMessage);
        uint256 c = a / b;
        // assert(a == b * c + a % b); // There is no case in which this doesn't hold

        return c;
    }
```

```
    /**
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
     * Reverts when dividing by zero.
     *
     * Counterpart to Solidity's `%` operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        return mod(a, b, "SafeMath: modulo by zero");
    }

    /**
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),
     * Reverts with custom message when dividing by zero.
     *
     * Counterpart to Solidity's `%` operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function mod(uint256 a, uint256 b, string memory errorMessage) internal pure returns (uint256) {
        require(b != 0, errorMessage);
        return a % b;
```

```
    }
}

contract Ownable {

    address private _owner;

    event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);

    /**
     * @dev Initializes the contract setting the deployer as the initial owner.
     */
    constructor () internal {
        _owner = msg.sender;
        emit OwnershipTransferred(address(0), msg.sender);
    }

    /**
     * @dev Returns the address of the current owner.
     */
    function owner() public view returns (address) {
        return _owner;
    }

    /**
     * @dev Throws if called by any account other than the owner.
     */
    modifier onlyOwner() {
        require(_owner == msg.sender, "YouSwap: CALLER_IS_NOT_THE_OWNER");
        _;
    }

    /**
```

```
     * @dev Leaves the contract without owner. It will not be possible to call
     * `onlyOwner` functions anymore. Can only be called by the current owner.
     *
     * NOTE: Renouncing ownership will leave the contract without an owner,
     * thereby removing any functionality that is only available to the owner.
     */
    function renounceOwnership() public virtual onlyOwner {
        emit OwnershipTransferred(_owner, address(0));
        _owner = address(0); //knownsec// 放弃 owner 权限
    }

    /**
     * @dev Transfers ownership of the contract to a new account (`newOwner`).
     * Can only be called by the current owner.
     */
    function transferOwnership(address newOwner) public virtual onlyOwner {
        require(newOwner != address(0), "YouSwap: NEW_OWNER_IS_THE_ZERO_ADDRESS");
        emit OwnershipTransferred(_owner, newOwner);
        _owner = newOwner; //knownsec// 转移 owner 权限至 newOwner
    }
}

interface ITokenYou {
    /**
     * @dev Returns the amount of tokens in existence.
     */
    function totalSupply() external view returns (uint256);

    /**
     * @dev Returns the amount of tokens owned by `account`.
     */
    function balanceOf(address account) external view returns (uint256);
```

```
/**
 * @dev Moves `amount` tokens from the caller's account to `recipient`.
 *
 * Returns a boolean value indicating whether the operation succeeded.
 *
 * Emits a {Transfer} event.
 */
function transfer(address recipient, uint256 amount) external returns (bool);

/**
 * @dev Returns the remaining number of tokens that `spender` will be
 * allowed to spend on behalf of `owner` through {transferFrom}. This is
 * zero by default.
 *
 * This value changes when {approve} or {transferFrom} are called.
 */
function allowance(address owner, address spender) external view returns (uint256);

/**
 * @dev Sets `amount` as the allowance of `spender` over the caller's tokens.
 *
 * Returns a boolean value indicating whether the operation succeeded.
 *
 * IMPORTANT: Beware that changing an allowance with this method brings the risk
 * that someone may use both the old and the new allowance by unfortunate
 * transaction ordering. One possible solution to mitigate this race
 * condition is to first reduce the spender's allowance to 0 and set the
 * desired value afterwards:
 * https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
 *
 * Emits an {Approval} event.
 */
```

```
    function approve(address spender, uint256 amount) external returns (bool);

    /**
     * @dev Moves `amount` tokens from `sender` to `recipient` using the
     * allowance mechanism. `amount` is then deducted from the caller's
     * allowance.
     *
     * Returns a boolean value indicating whether the operation succeeded.
     *
     * Emits a {Transfer} event.
     */
    function transferFrom(address sender, address recipient, uint256 amount) external returns (bool);

    /**
     * @dev Emitted when `value` tokens are moved from one account (`from`) to
     * another (`to`).
     *
     * Note that `value` may be zero.
     */
    event Transfer(address indexed from, address indexed to, uint256 value);

    /**
     * @dev Emitted when the allowance of a `spender` for an `owner` is set by
     * a call to {approve}. `value` is the new allowance.
     */
    event Approval(address indexed owner, address indexed spender, uint256 value);

    event MaxSupplyChanged(uint256 oldValue, uint256 newValue);

    function resetMaxSupply(uint256 newValue) external;

    function mint(address recipient, uint256 amount) external;
```

```
    function burn(uint256 amount) external;

    function burnFrom(address account, uint256 amount) external;
}

contract TokenYou is Ownable, ITokenYou {
    using SafeMath for uint256;

    string private constant _name = 'YouSwap';
    string private constant _symbol = 'YOU';
    uint8 private constant _decimals = 6; //knownsec// 默认代币精度为6
    uint256 private _totalSupply;
    uint256 private _transfers; //knownsec// 存储代币转账次数
    uint256 private _holders; //knownsec// 存储代币持有者数量
    uint256 private _maxSupply;
    mapping(address => uint256) private _balanceOf;
    mapping(address => mapping(address => uint256)) private _allowances;

    mapping(address => uint8) private _minters;

    constructor() public {
        _totalSupply = 0;
        _transfers = 0;
        _holders = 0;
        _maxSupply = 2 * 10 ** 14;
    }

    /**
     * @dev Returns the name of the token.
     */
    function name() public pure returns (string memory) {
        return _name;
```

```
}

/**
 * @dev Returns the symbol of the token, usually a shorter version of the
 * name.
 */
function symbol() public pure returns (string memory) {
    return _symbol;
}

/**
 * @dev Returns the number of decimals used to get its user representation.
 * For example, if `decimals` equals `2`, a balance of `505` tokens should
 * be displayed to a user as `5,05` (`505 / 10 ** 2`).
 *
 * Tokens usually opt for a value of 18, imitating the relationship between
 * Ether and Wei. This is the value {ERC20} uses, unless {_setupDecimals} is
 * called.
 *
 * NOTE: This information is only used for _display_ purposes: it in
 * no way affects any of the arithmetic of the contract, including
 * {ITokenYou-balanceOf} and {ITokenYou-transfer}.
 */
function decimals() public pure returns (uint8) {
    return _decimals;
}

/**
 * @dev See {ITokenYou-totalSupply}.
 */
function totalSupply() public view override returns (uint256) {
    return _totalSupply;
}
```

```
 /**
* @dev See {ITokenYou-maxSupply}.
*/
 function maxSupply() public view returns (uint256) {
        return _maxSupply;
 }

 function transfers() public view returns (uint256) {
        return _transfers;
 }

 function holders() public view returns (uint256) {
        return _holders;
 }

 /**
   * @dev See {ITokenYou-balanceOf}.
   */
 function balanceOf(address account) public view override returns (uint256) {
        return _balanceOf[account];
 }

 /**
   * @dev See {ITokenYou-transfer}.
   *
   * Requirements:
   *
   * - `recipient` cannot be the zero address.
   * - the caller must have a balance of at least `amount`.
   */
 function transfer(address recipient, uint256 amount) public virtual override returns (bool) {
        _transfer(msg.sender, recipient, amount);
```

```
        return true;
    }

    /**
     * @dev See {ITokenYou-allowance}.
     */
    function allowance(address owner, address spender) public view virtual override returns (uint256) {
        return _allowances[owner][spender];
    }

    /**
     * @dev See {ITokenYou-approve}.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     */
    function approve(address spender, uint256 amount) public override returns (bool) {
        _approve(msg.sender, spender, amount);
        return true;
    }

    /**
     * @dev See {ITokenYou-transferFrom}.
     *
     * Emits an {Approval} event indicating the updated allowance. This is not
     * required by the EIP. See the note at the beginning of {ERC20}.
     *
     * Requirements:
     *
     * - `sender` and `recipient` cannot be the zero address.
     * - `sender` must have a balance of at least `amount`.
```

```
     * - the caller must have allowance for ``sender``'s tokens of at least
     * `amount`.
     */
    function transferFrom(address sender, address recipient, uint256 amount) public override returns (bool) {
        _transfer(sender, recipient, amount);
        _approve(sender, msg.sender, _allowances[sender][msg.sender].sub(amount, "YouSwap: TRANSFER_AMOUNT_EXCEEDS_ALLOWANCE"));
        return true;
    }

    /**
     * @dev Atomically increases the allowance granted to `spender` by the caller.
     *
     * This is an alternative to {approve} that can be used as a mitigation for
     * problems described in {ITokenYou-approve}.
     *
     * Emits an {Approval} event indicating the updated allowance.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     */
    function increaseAllowance(address spender, uint256 addedValue) public returns (bool) {
        _approve(msg.sender, spender, _allowances[msg.sender][spender].add(addedValue));
        return true;
    }

    /**
     * @dev Atomically decreases the allowance granted to `spender` by the caller.
     *
     * This is an alternative to {approve} that can be used as a mitigation for
     * problems described in {ITokenYou-approve}.
```

```
     *
     * Emits an {Approval} event indicating the updated allowance.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     * - `spender` must have allowance for the caller of at least
     * `subtractedValue`.
     */
    function decreaseAllowance(address spender, uint256 subtractedValue) public returns (bool) {
        _approve(msg.sender, spender, _allowances[msg.sender][spender].sub(subtractedValue,
"YouSwap: DECREASED_ALLOWANCE_BELOW_ZERO"));
        return true;
    }

    /**
     * @dev Moves tokens `amount` from `sender` to `recipient`.
     *
     * This is internal function is equivalent to {transfer}, and can be used to
     * e.g. implement automatic token fees, slashing mechanisms, etc.
     *
     * Emits a {Transfer} event.
     *
     * Requirements:
     *
     * - `sender` cannot be the zero address.
     * - `recipient` cannot be the zero address.
     * - `sender` must have a balance of at least `amount`.
     */
    function _transfer(address sender, address recipient, uint256 amount) internal {
        //knownsec// 零地址检查
        require(sender != address(0), "YouSwap:
TRANSFER_FROM_THE_ZERO_ADDRESS");
```

```
        require(recipient != address(0), "YouSwap: TRANSFER_TO_THE_ZERO_ADDRESS");
        require(amount > 0, "YouSwap: TRANSFER_ZERO_AMOUNT"); //knownsec// 转账数量限制

        if(_balanceOf[recipient] == 0) _holders++; //knownsec// 当接收地址代币余额为空时更新代币持有者数量
        //knownsec// 更新转账双方代币余额
        _balanceOf[sender] = _balanceOf[sender].sub(amount, "YouSwap: TRANSFER_AMOUNT_EXCEEDS_BALANCE");
        _balanceOf[recipient] = _balanceOf[recipient].add(amount);

        _transfers ++; //knownsec// 更新转账次数

        if (_balanceOf[sender] == 0) _holders--; //knownsec// 当转账后发送者地址代币余额为空时减少代币持有者数量

        emit Transfer(sender, recipient, amount);
    }

    /**
     * @dev Destroys `amount` tokens from `account`, reducing the
     * total supply.
     *
     * Emits a {Transfer} event with `to` set to the zero address.
     *
     * Requirements:
     *
     * - `account` cannot be the zero address.
     * - `account` must have at least `amount` tokens.
     */
    function _burn(address account, uint256 amount) internal {
        require(account != address(0), "YouSwap: BURN_FROM_THE_ZERO_ADDRESS"); //knownsec// 零地址检查
```

```
        require(_balanceOf[account] > 0, "YouSwap: INSUFFICIENT_FUNDS"); //knownsec// 地址余额检查

        _balanceOf[account] = _balanceOf[account].sub(amount, "YouSwap: BURN_AMOUNT_EXCEEDS_BALANCE");
        if (_balanceOf[account] == 0) _holders --; //knownsec// 当代币销毁后销毁地址代币余额为空时减少代币持有者数量
        _totalSupply = _totalSupply.sub(amount); //knownsec// 更新代币总量
        _transfers++; //knownsec// 增加转账次数
        emit Transfer(account, address(0), amount);
    }

    /**
     * @dev Sets `amount` as the allowance of `spender` over the `owner`s tokens.
     *
     * This internal function is equivalent to `approve`, and can be used to
     * e.g. set automatic allowances for certain subsystems, etc.
     *
     * Emits an {Approval} event.
     *
     * Requirements:
     *
     * - `owner` cannot be the zero address.
     * - `spender` cannot be the zero address.
     */
    function _approve(address owner, address spender, uint256 amount) internal {
        //knownsec// 零地址检查
        require(owner != address(0), "YouSwap: APPROVE_FROM_THE_ZERO_ADDRESS");
        require(spender != address(0), "YouSwap: APPROVE_TO_THE_ZERO_ADDRESS");

        _allowances[owner][spender] = amount; //knownsec// 修改授权值
        emit Approval(owner, spender, amount);
    }
```

```
    /**
     * @dev Destroys `amount` tokens from the caller.
     *
     * See {TokenYou-_burn}.
     */
    function burn(uint256 amount) external override {
        _burn(msg.sender, amount); //knownsec// 销毁调用者一定数量的代币
    }

    /**
     * @dev Destroys `amount` tokens from `account`, deducting from the caller's
     * allowance.
     *
     * See {TokenYou-_burn} and {TokenYou-allowance}.
     *
     * Requirements:
     *
     * - the caller must have allowance for ``accounts``'s tokens of at least
     * `amount`.
     */
    function burnFrom(address account, uint256 amount) external override {
        uint256 decreasedAllowance = allowance(account, msg.sender).sub(amount, "YouSwap:
BURN_AMOUNT_EXCEEDS_ALLOWANCE");

        _approve(account, msg.sender, decreasedAllowance); //knownsec// 修改授权值
        _burn(account, amount); //knownsec// 代理销毁授权地址一定数量的代币
    }
    //knownsec// 限制仅可有铸币权限的用户进行铸币
    modifier isMinter() {
        require(_minters[msg.sender] == 1, "YouSwap: IS_NOT_A_MINTER");
        _;
    }
```

```
    function isContract(address account) internal view returns (bool) {
        uint256 size;
        assembly {size := extcodesize(account)}
        return size > 0;
    }

    function mint(address recipient, uint256 amount) external override isMinter {
        require(_totalSupply.add(amount) <= _maxSupply, 'YouSwap: EXCEEDS_MAX_SUPPLY'); //knownsec// 铸币限制，铸币后代币总量不可超过最大铸币数量
        _totalSupply = _totalSupply.add(amount); //knownsec// 更新代币总量

        if (_balanceOf[recipient] == 0) _holders++; //knownsec// 当铸币地址余额为空时更新代币持有者数量
        _balanceOf[recipient] = _balanceOf[recipient].add(amount); //knownsec// 修改铸币地址代币余额

        _transfers++; //knownsec// 增加转账次数
        emit Transfer(address(0), recipient, amount);
    }

    function addMinter(address account) external onlyOwner {
        require(isContract(account), "YouSwap: MUST_BE_A_CONTRACT_ADDRESS");
        _minters[account] = 1; //knownsec// 授予指定地址铸币权限
    }

    function removeMinter(address account) external onlyOwner{
        _minters[account] = 0; //knownsec// 撤销指定地址铸币权限
    }

    function resetMaxSupply(uint256 newValue) external override onlyOwner{
        require(newValue > _totalSupply && newValue< _maxSupply, 'YouSwap: NOT_ALLOWED'); //knownsec// 该代币可实现铸币；通过 owner 控制，铸币上限可修改（仅
```

```
可调小）
        emit MaxSupplyChanged(_maxSupply,newValue);
        _maxSupply = newValue; //knownsec//  变更最大铸币数量
    }
}
```

安全建议：无。

4. 代码基本漏洞检测

4.1. 编译器版本安全【通过】

检查合约代码实现中是否使用了安全的编译器版本

检测结果：经检测，智能合约代码中指定了 IDO 合约编译器版本为 0.5.16，TokenYou 合约编译器版本为 0.6.0 以上，不存在该安全问题。。

安全建议：无。

4.2. 冗余代码【通过】

检查合约代码实现中是否包含冗余代码

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.3. 安全算数库的使用【通过】

检查合约代码实现中是否使用了 SafeMath 安全算数库

检测结果：经检测，智能合约代码中已使用 SafeMath 安全算数库，不存在该安全问题。

安全建议：无。

4.4. 不推荐的编码方式【通过】

检查合约代码实现中是否有官方不推荐或弃用的编码方式

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.5. require/assert 的合理使用【通过】

检查合约代码实现中 require 和 assert 语句使用的合理性

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.6. fallback 函数安全【通过】

检查合约代码实现中是否正确使用 fallback 函数

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.7. tx.origin 身份验证【通过】

tx.origin 是 Solidity 的一个全局变量，它遍历整个调用栈并返回最初发送调用（或事务）的帐户的地址。在智能合约中使用此变量进行身份验证会使合约容易受到类似网络钓鱼的攻击。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.8. owner 权限控制【通过】

检查合约代码实现中的 owner 是否具有过高的权限。例如，任意修改其他账户余额等。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.9. gas 消耗检测【通过】

检查 gas 的消耗是否超过区块最大限制

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.10. call 注入攻击【通过】

call 函数调用时，应该做严格的权限控制，或直接写死 call 调用的函数。

检测结果：经检测，智能合约未使用 call 函数，不存在此漏洞。

安全建议：无。

4.11. 低级函数安全【通过】

检查合约代码实现中低级函数（call/delegatecall）的使用是否存在安全漏洞

call 函数的执行上下文是在被调用的合约中；而 delegatecall 函数的执行上下文是在当前调用该函数的合约中

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.12. 增发代币漏洞【通过】

检查在初始化代币总量后，代币合约中是否存在可能使代币总量增加的函数。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.13. 访问控制缺陷检测【通过】

合约中不同函数应设置合理的权限

检查合约中各函数是否正确使用了 public、private 等关键词进行可见性修饰，检查合约是否正确定义并使用了 modifier 对关键函数进行访问限制，避免越权导致的问题。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.14. 数值溢出检测【通过】

智能合约中的算数问题是指整数溢出和整数下溢。

Solidity 最多能处理 256 位的数字（2^256-1），最大数字增加 1 会溢出得到 0。同样，当数字为无符号类型时，0 减去 1 会下溢得到最大数字值。

整数溢出和下溢不是一种新类型的漏洞，但它们在智能合约中尤其危险。溢出情况会导致不正确的结果，特别是如果可能性未被预期，可能会影响程序的可

靠性和安全性。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.15. 算术精度误差【通过】

Solidity 作为一门编程语言具备和普通编程语言相似的数据结构设计，比如：变量、常量、函数、数组、函数、结构体等等，Solidity 和普通编程语言也有一个较大的区别——Solidity 没有浮点型，且 Solidity 所有的数值运算结果都只会是整数，不会出现小数的情况，同时也不允许定义小数类型数据。合约中的数值运算必不可少，而数值运算的设计有可能造成相对误差，例如同级运算：5/2*10=20，而 5*10/2=25，从而产生误差，在数据更大时产生的误差也会更大，更明显。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.16. 错误使用随机数【通过】

智能合约中可能需要使用随机数，虽然 Solidity 提供的函数和变量可以访问明显难以预测的值，如 block.number 和 block.timestamp，但是它们通常或者比看起来更公开，或者受到矿工的影响，即这些随机数在一定程度上是可预测的，所以恶意用户通常可以复制它并依靠其不可预知性来攻击该功能。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.17. 不安全的接口使用【通过】

检查合约代码实现中是否使用了不安全的接口

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.18. 变量覆盖【通过】

检查合约代码实现中是否存在变量覆盖导致的安全问题

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.19. 未初始化的储存指针【通过】

在 solidity 中允许一个特殊的数据结构为 struct 结构体，而函数内的局部变量默认使用 storage 或 memory 储存。

而存在 storage(存储器)和 memory(内存)是两个不同的概念，solidity 允许指针指向一个未初始化的引用，而未初始化的局部 stroage 会导致变量指向其他储存变量，导致变量覆盖，甚至其他更严重的后果，在开发中应该避免在函数中初始化 struct 变量。

检测结果：经检测，智能合约代码不使用结构体，不存在该问题。

安全建议：无。

4.20. 返回值调用验证【通过】

此问题多出现在和转币相关的智能合约中，故又称作静默失败发送或未经检

查发送。

在 Solidity 中存在 transfer()、send()、call.value()等转币方法，都可以用于向某一地址发送 Ether，其区别在于： transfer 发送失败时会 throw，并且进行状态回滚；只会传递 2300gas 供调用，防止重入攻击；send 发送失败时会返回 false；只会传递 2300gas 供调用，防止重入攻击；call.value 发送失败时会返回 false；传递所有可用 gas 进行调用（可通过传入 gas_value 参数进行限制），不能有效防止重入攻击。

如果在代码中没有检查以上 send 和 call.value 转币函数的返回值，合约会继续执行后面的代码，可能由于 Ether 发送失败而导致意外的结果。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.21. 交易顺序依赖【通过】

由于矿工总是通过代表外部拥有地址（EOA）的代码获取 gas 费用，因此用户可以指定更高的费用以便更快地开展交易。由于以太坊区块链是公开的，每个人都可以看到其他人未决交易的内容。这意味着，如果某个用户提交了一个有价值的解决方案，恶意用户可以窃取该解决方案并以较高的费用复制其交易，以抢占原始解决方案。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.22. 时间戳依赖攻击【通过】

数据块的时间戳通常来说都是使用矿工的本地时间，而这个时间大约能有 900 秒的范围波动，当其他节点接受一个新区块时，只需要验证时间戳是否晚于之前的区块并且与本地时间误差在 900 秒以内。一个矿工可以通过设置区块的时间戳来尽可能满足有利于他的条件来从中获利。

检查合约代码实现中是否存在有依赖于时间戳的关键功能

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.23. 拒绝服务攻击【通过】

在以太坊的世界中，拒绝服务是致命的，遭受该类型攻击的智能合约可能永远无法恢复正常工作状态。导致智能合约拒绝服务的原因可能有很多种，包括在作为交易接收方时的恶意行为，人为增加计算功能所需 gas 导致 gas 耗尽，滥用访问控制访问智能合约的 private 组件，利用混淆和疏忽等等。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.24. 假充值漏洞【通过】

在代币合约的 transfer 函数对转账发起人(msg.sender)的余额检查用的是 if 判断方式，当 balances[msg.sender] < value 时进入 else 逻辑部分并 return false，最终没有抛出异常，我们认为仅 if/else 这种温和的判断方式在 transfer 这类敏感函数场景中是一种不严谨的编码方式。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.25. 重入攻击检测【通过】

重入漏洞是最著名的以太坊智能合约漏洞，曾导致了以太坊的分叉（The DAO hack）。

Solidity 中的 call.value()函数在被用来发送 Ether 的时候会消耗它接收到的所有 gas，当调用 call.value()函数发送 Ether 的操作发生在实际减少发送者账户的余额之前时，就会存在重入攻击的风险。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

4.26. 重放攻击检测【通过】

合约中如果涉及委托管理的需求，应注意验证的不可复用性，避免重放攻击

在资产管理体系中，常有委托管理的情况，委托人将资产给受托人管理，委托人支付一定的费用给受托人。这个业务场景在智能合约中也比较普遍。。

检测结果：经检测，智能合约未使用 call 函数，不存在此漏洞。

安全建议：无。

4.27. 重排攻击检测【通过】

重排攻击是指矿工或其他方试图通过将自己的信息插入列表(list)或映射(mapping)中来与智能合约参与者进行“竞争”，从而使攻击者有机会将自己的

信息存储到合约中。

检测结果:经检测，智能合约代码中不存在相关漏洞。

安全建议:无。

5. 附录 A：合约代码

本次测试代码来源：

TokenYou
https://etherscan.io/address/0x1d32916cfa6534d261ad53e2498ab95505bd2510#code
IDO
https://etherscan.io/address/0x59e6639bef44164ba44aa58771b94df30bc023a6#code

6. 附录 B：安全风险评级标准

智能合约漏洞评级标准	
漏洞评级	**漏洞评级说明**
高危漏洞	能直接造成代币合约或用户资金损失的漏洞，如：能造成代币价值归零的数值溢出漏洞、能造成交易所损失代币的假充值漏洞、能造成合约账户损失 ETH 或代币的重入漏洞等； 能造成代币合约归属权丢失的漏洞，如：关键函数的访问控制缺陷、call 注入导致关键函数访问控制绕过等； 能造成代币合约无法正常工作的漏洞，如：因向恶意地址发送 ETH 导致的拒绝服务漏洞、因 gas 耗尽导致的拒绝服务漏洞。
中危漏洞	需要特定地址才能触发的高风险漏洞，如代币合约拥有者才能触发的数值溢出漏洞等；非关键函数的访问控制缺陷、不能造成直接资金损失的逻辑设计缺陷等。
低危漏洞	难以被触发的漏洞、触发之后危害有限的漏洞，如需要大量 ETH 或代币才能触发的数值溢出漏洞、触发数值溢出后攻击者无法直接获利的漏洞、通过指定高 gas 触发的事务顺序依赖风险等。

7. 附录 C：智能合约安全审计工具简介

7.1 Manticore

Manticore 是一个分析二进制文件和智能合约的符号执行工具，Manticore 包含一个符号以太坊虚拟机（EVM），一个 EVM 反汇编器/汇编器以及一个用于自动编译和分析 Solidity 的方便界面。它还集成了 Ethersplay，用于 EVM 字节码的 Bit of Traits of Bits 可视化反汇编程序，用于可视化分析。 与二进制文件一样，Manticore 提供了一个简单的命令行界面和一个用于分析 EVM 字节码的 Python API。

7.2 Oyente

Oyente 是一个智能合约分析工具，Oyente 可以用来检测智能合约中常见的 bug，比如 reentrancy、事务排序依赖等等。更方便的是，Oyente 的设计是模块化的，所以这让高级用户可以实现并插入他们自己的检测逻辑，以检查他们的合约中自定义的属性。

7.3 securify.sh

Securify 可以验证以太坊智能合约常见的安全问题，例如交易乱序和缺少输入验证，它在全自动化的同时分析程序所有可能的执行路径，此外，Securify 还具有用于指定漏洞的特定语言，这使 Securify 能够随时关注当前的安全性和其他可靠性问题。

7.4 Echidna

Echidna 是一个为了对 EVM 代码进行模糊测试而设计的 Haskell 库。

7.5 MAIAN

MAIAN 是一个用于查找以太坊智能合约漏洞的自动化工具，Maian 处理合

约的字节码，并尝试建立一系列交易以找出并确认错误。

7.6 ethersplay

ethersplay 是一个 EVM 反汇编器，其中包含了相关分析工具。

7.7 ida-evm

ida-evm 是一个针对以太坊虚拟机（EVM）的 IDA 处理器模块。

7.8 Remix-ide

Remix 是一款基于浏览器的编译器和 IDE，可让用户使用 Solidity 语言构建以太坊合约并调试交易。

7.9 知道创宇区块链安全审计人员专用工具包

知道创宇渗透测试人员专用工具包，由知道创宇渗透测试工程师研发，收集和使用，包含专用于测试人员的批量自动测试工具，自主研发的工具、脚本或利用工具等。

知道创宇

北京知道创宇信息技术股份有限公司

咨询电话 +86(10)400 060 9587

邮　　箱 sec@knownsec.com

官　　网 www.knownsec.com

地　　址 北京市 朝阳区 望京 SOHO T2-B座-2509