HLWGroup
AUDIT SERVICE

INITIAL AUDIT

PSYOP

Audited on May 17th 2023

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

SMART CONTRACT AUDIT SERVICES REPORT
PSYOP

Summary

This document was commissioned by PSYOP (https://twitter/psyopeth) for the express reason to audit the project's affiliated smart contracts.

HLW Group is not promoting PSYOP under any circumstances. Please see the Disclaimer section of this document for more details.

PSYOP is an ERC20 token that will be launched on the Ethereum Blockchain using the Uniswap router.

HLWGroup
AUDIT SERVICE

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Table of Contents

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Project Summary

Project Name	PSYOP
Intended Network	ETHEREUM
Language / Version	SOLIDITY Version >=0.8.0<0.9.0
Codebase Location	https://github.com/psyop/psyop-sc
Initial Commit Audited	f51e38ede8f0c90eaf16a5d4ef9b119d02b4669a
Final Commit Audited	22c5ef789f916c368b47ebc57d1faaf458a37323

Audit Summary

Requested Date	5/16/2023
Delivery Date	5/18/2023
Audit Methodology	Static Analysis, Manual Review

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Preliminary Audit Scope

The scope of this audit was limited to the smart contract(s) shown below.

Contract Name	Abbreviation	Checksum Value
Psyop.sol	PSY1	7bd79ad56c668b9e9989ee8e8ceb2f8cc30c9048d4ac8020449754be20c30996
Restrictable.sol	PSY2	3bbf81ffcabe586f8b29d4fc831812e099fffb053f49e6753be55167c402e1e0

The 'Checksum' value is a placeholder for the state of the contract at the time the snapshot was taken for the audit. HLW Group leverages sha256sum to calculate this value.

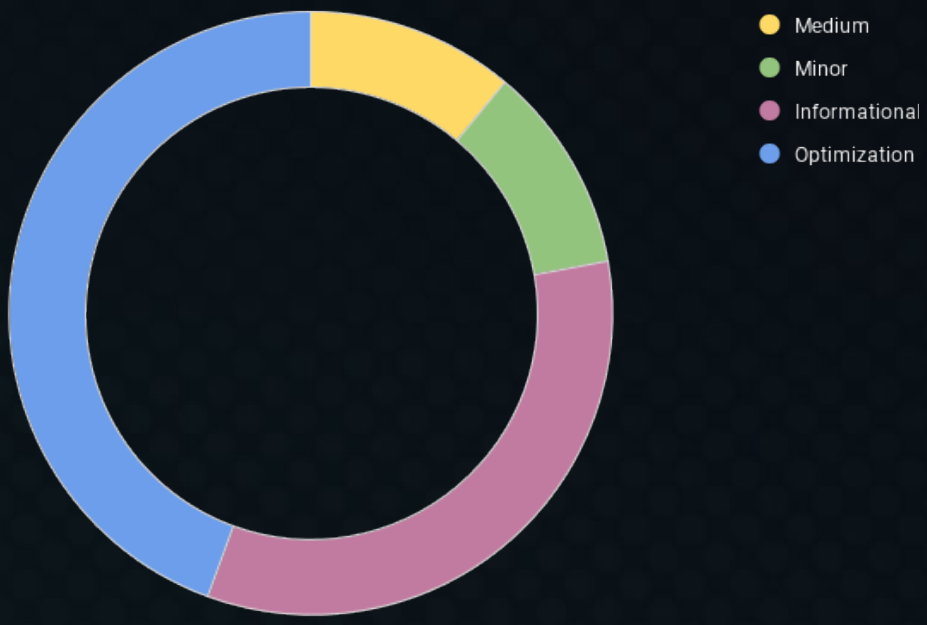
- Restrictable.sol is an abstract solidity contract that controls a _restricted boolean and has several helper methods and modifiers to check for the value and update it.
- Psyop.sol is an ERC20 token using OpenZeppelins Ownable module; it has blacklist, pause, anti bot and buy limit functionality.
- The contract has a max buy limit of 137,500,000 tokens in a single transaction.
- The contract has a total supply of 550,000,000,000 tokens.
- The contract will send initial minted tokens to 1 address supplied in the constructor.
- There is a whitelist for bypassing pause and anti bot functionality.
- The owner can add or remove addresses from the whitelist..
- The owner can pause and unpause the contract at any time.
- The owner can set the uniswap pool contract address.
- The owner can turn anti bot and buy limits off.
- If a user is blacklisted, they can no longer transfer tokens.

HLWGroup
AUDIT SERVICE

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Preliminary Summary of Findings

HLW Group has detected the following issues during the smart contract audit process. PSYOP should address Critical and Major issues ASAP to prevent loss.



Vulnerability Summary

Level	Total	Pending	Declined	Ack'd	Mitigated	Part Res	Resolved
Critical	0	0	0	0	0	0	0
Major	0	0	0	0	0	0	0
Medium	1	0	0	0	0	0	1
Minor	1	0	0	1	0	0	0
Optimization	4	0	0	0	0	0	4
Informational	3	0	0	2	0	0	1

HLWGroup
AUDIT SERVICE

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Preliminary Detailed Explanations and Potential Remedies

PSY1-01

Level	Category	Location	Status
Medium	Logic	Psyop.sol:95-97 Psyop.sol:130-177	Resolved

Description

Transfers will always revert if deadBlock is set to a block in the future, and can be set to an arbitrary value by the owner.

The owner has the ability to set the deadBlock field providing the _currentBlock and _numberOfDeadBlocks as input, instead of relying on block.number and a fixed number of blocks to last for.

```
function setDeadBlock(uint256 _currentBlock, uint256 _numberOfDeadblocks) public onlyOwner {
  deadBlock = _currentBlock + _numberOfDeadblocks; // setting up our own customer number instead of it being fixed.
}
```

If the deadBlock is accidentally or maliciously set too high, all trading will be disabled for non whitelisted users until block.number is higher than deadBlock

```
if (_isBuyTokenTransfer(sender, recipient)) {
  if (shouldBlacklist && _checkIfBot(recipient) && !isBlacklist(recipient)) {
    _setAddressToBlackList(recipient, true);
  }
  if (restricted() && amount > MAX_BUY) {
    revert LimitExceeded();
  }
  _lastBlockTransfer[recipient] = block.number; // could cost more gas to purchase...
}

if (_isSellTokenTransfer(recipient, amount) && block.number <= _lastBlockTransfer[recipient]) {
  revert NotAllowed();
}
```

During a buy, a _checkIfBot function is called and if the user is not whitelisted and if *either* they are a contract *or* they trade before deadBlock., the address is subsequently added to the blacklist mapping.

```
function _checkIfBot(address _address) internal view returns (bool) {
  return (block.number < deadBlock || _isContract(_address)) && !isWhitelist(_address);
}
```

Further on after bot checks are done, the _isAllowedToTransfer function is checked. This checks if either the sender or receiver are blacklisted and will revert the transaction.

```
function _isAllowedToTransfer(address sender, address recipient) internal view returns (bool) {
  return (recipient == address(0) || (!isBlacklist(recipient) && !isBlacklist(sender)));
}
```

This also means that writing to storage just to revert does nothing as no data is stored on chain in a revert, and is an unnecessary gas cost.

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Recommendation

- Replace _setAddressToBlackList(recipient, true) with a revert.
- Set a fixed number of blocks to use for _setDeadBlock() and use block.number as your starting block

  This will revert the transaction earlier instead, avoids storage reads and writes and allows you to remove a blacklist check.

PSY1-02

Level	Category	Location	Status
Optimization	Syntax	Psyop.sol:139	Resolved

Description

isBlacklist is a public function. In Solidity, it is cheaper to access a storage slot directly instead of redirecting via public methods.

```
function _isAllowedToTransfer(address sender, address recipient) internal view returns (bool) {
  return (recipient == address(0) || (!isBlacklist(recipient) && !isBlacklist(sender)));
}
```

Recommendation

- Replace isBlacklist(recipient) with blackList[recipient].
- Replace isBlacklist(sender) with blackList[sender].

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

PSY1-03

Level	Category	Location	Status
Optimization	Syntax	Psyop.sol:135	Resolved

Description

isWhitelist is a public function that reads from the whitelist storage. In Solidity, it is cheaper to access a storage slot directly instead of redirecting via public methods.

```
function _checkIfBot(address _address) internal view returns (bool) {
  return (block.number < deadBlock || _isContract(_address)) && !isWhitelist(_address);
}
```

Recommendation

- Replace isWhitelist(_address) with whiteList[_address].

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

PSY1-04

Level	Category	Location	Status
Optimization	Logic/Syntax	Psyop.sol:172	Resolved

Description

Whitelisting sender address 0 here is extraneous because the only minting is done during deployment of the contract when paused is false.

```
if (paused() && (!isWhitelist(sender) || !isWhitelist(recipient) || sender != address(0))) {
  revert ContractPaused();
}
```

Recommendation

- Remove reference to sender != address(0).

PSY1-05

Level	Category	Location	Status
Informational	Constant	Psyop.sol:29	Acknowledged

Description

MAX_BUY is currently set to 137,500,000 tokens. This value will be unchangeable after deployment.

```
uint256 public constant MAX_BUY = 137_500_000 ether;
```

Recommendation

- We suggest replacing the constant with a setter so that the maximum buy can be changed in the future if desired.

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

PSY1-06

Level	Category	Location	Status
Minor	Logic	Psyop.sol:135 Psyop.sol:172	Acknowledged

Description

The whitelist field is used for multiple purposes. It allows the user to bypass both the pause functionality and the bot check functionality.
This could lead to unintended addresses being able to trade when the contract is paused.

```
function _checkIfBot(address _address) internal view returns (bool) {
  return (block.number < deadBlock || _isContract(_address)) && !isWhitelist(_address);
}
```

```
if (paused() && (!isWhitelist(sender) || !isWhitelist(recipient) || sender != address(0))) {
  revert ContractPaused();
}
```

Recommendation

- Use (2) separate whitelist storage fields to separate logic.

PSY1-07

Level	Category	Location	Status
Informational	Logic	Psyop.sol:155-157	Acknowledged

Description

The amount variable can never go below zero as it is an unsigned integer (uint256). There is no effect on allowing transfers with 0 amounts so no need to restrict it.

```
function _beforeTokenTransfer(address sender, address recipient, uint256 amount) internal override {
  if (amount <= 0) {
    revert LessThanZero();
  }
```

Recommendation

- Remove unnecessary code. Alternatively, only check for amount == 0, if 0 reverts are desired.

PSY1-08

Level	Category	Location	Status
Informational	Logic	Psyop.sol:96	Resolved

Description

Internal method usage can be simplified to storage access for simplicity if all they do is write variables.

```
function _setAddressToBlackList(address _address, bool _allow) private {
  blackList[_address] = _allow;
}
```

```
function setAddressToBlackList(address _address, bool _allow) public onlyOwner {
  _setAddressToBlackList(_address, _allow);
}
```

Recommendation

- Use blacklist[_address] = true instead.

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

PSY2-01

Level	Category	Location	Status
Optimization	Logic	Restrictable.sol file	Resolved

Description

The Restrictable.sol class is used for nothing more than a boolean check in this contract, extra code is unnecessary.

```
/**
 * @dev Returns true if the contract is restricted, and false otherwise.
 */
function restricted() public view virtual returns (bool) {
    return _restricted;
}
```

```
if (restricted() && amount > MAX_BUY) {
  revert LimitExceeded();
}
```

```
function restrict() public onlyOwner {
  _restrict();
}

function unrestrict() public onlyOwner {
  _unrestrict();
}
```

Recommendation

- The Restrictable.sol can be replaced with simpler boolean logic inside the main token contract.

HLWGroup
AUDIT SERVICE

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Final Audit Scope

Contract Name	Abbreviation	Checksum Value
Psyop.sol	PSYF1	055becf2dda0471e93ece30e7e4195eb6a3401e89583533b899b652e30c50ba4

The 'Checksum' value is a placeholder for the state of the contract at the time the snapshot was taken for the audit. HLW Group leverages sha256sum to calculate this value.

- Psyop.sol is an ERC20 token using OpenZeppelins Ownable module; it has pause, anti bot and buy limit functionality.
- The contract has a max buy limit of 137,500,000 tokens in a single transaction.
- The contract has a total supply of 550,000,000,000 tokens.
- The contract will split initial minted tokens up to 2 addresses:
  - 522,500,000,000 to the address supplied in the constructor
  - 27,500,000,000 to the deployer address
- There is a whitelist for bypassing pause and anti bot functionality.
- The owner can add or remove addresses from the whitelist.
- The contract has an unleashPsyop function that can only be called by the owner.
  - When this is called, all pause, anti bot and buy limit functionality is disabled forever and ownership is renounced.
- The owner can pause and unpause the contract at any time.
  - When unpaused, there is a (3) block countdown in which every buy will revert.
- The owner can set the Uniswap pool contract address.
- The owner can turn anti-bot and buy limits off.
- The contract implements _lastBlockTransfer storage to keep track of when an address last bought or sold.
  - This limits trades to only allow for 1 buy or 1 sell per transaction per address.

HLWGroup
AUDIT SERVICE

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Final Summary of Findings

HLW Group has detected the following issues during the smart contract audit process. PSYOP should address Critical and Major issues ASAP to prevent loss.

Vulnerability Summary

Level	Total	Pending	Declined	Ack'd	Mitigated	Part Res	Resolved
Critical	0	0	0	0	0	0	0
Major	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0
Minor	1	0	0	1	0	0	0
Optimization	0	0	0	0	0	0	0
Informational	0	0	0	0	0	0	0

Final Detailed Explanations and Potential Remedies

PSYF1-01

Level	Category	Location	Status
Minor	Logic	Psyop.sol:145 Psyop.sol:166	Acknowledged

Description

The whitelist field is used for multiple purposes. It allows the user to bypass both the pause functionality and the bot check functionality.
This could lead to unintended addresses being able to trade when the contract is paused.

```
/**
 * Checks if address has inhuman reflexes or if it's a contract
 * @param _address Address in question
 */
function _checkIfBot(address _address) internal view returns (bool) {
  return (block.number < DEADBLOCK_COUNT + deadblockStart || _isContract(_address)) && !whitelist[_address];
}
```

```
if (paused() && !whitelist[sender]) { revert ContractPaused(); }
```

Recommendation

- Use (2) separate whitelist storage fields to separate logic.

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without HLW Group's prior written consent in each instance.

This report is not, nor should it be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should it be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts HLW Group to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor does it provide any indication of the technology's proprietors, business, business model, or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice and should not be leveraged as such. This report represents an extensive assessment process intended to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. HLW Group's position is that each company and individual are responsible for their own due diligence and continuous security. HLW Group's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by HLW Group are subject to dependencies and are under continuous development. You agree that your access and/or use, including but not limited to any services, reports, or materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access and depend upon multiple layers of third parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, HLW GROUP HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, HLW GROUP SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, HLW GROUP MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, HLW GROUP PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER HLW GROUP NOR ANY OF HLW GROUP'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. HLW GROUP WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT HLW GROUP'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST HLW GROUP WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF HLW GROUP CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF THE CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST HLW GROUP WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Our Vision for Smart Contract Auditing

- Provide accurate reviews.
- Provide insights on how to remedy any findings.
- Provide flexible options for low-cap project owners.

Contact Us At:
audit@hlwgroup.dev
https://hlwgroup.dev/

Our team of engineers have built dozens of products such as:

- Our own Cross-Chain DEX
- Cross-Chain Bridging Solution
- Several Blockchain Games
- NFT Auction House
- Dozens of Tokens ranging all major EIP Standards
- Much more...