



# WATCHDOG

## SECRET SCANNING ENGINE



Team Uncensored

# ✦ WHAT DOES WATCHDOG DO? ✦

Our Secrets Scanning Engine is a powerful tool designed for cybersecurity professionals and developers to detect potential leaks of sensitive information such as authentication tokens, API keys, and private cryptographic keys. It serves as a crucial asset throughout the software development lifecycle, from pre-deployment to post-deployment phases.

This comprehensive solution employs both active and passive scanning techniques to thoroughly examine local directories and online repositories where code may be deployed or pushed.



# WHY USE US (FEATURES)



- ✧ Passive Scans and Active Real Time Scans.
- ✧ Scan entire codebases at once with our fast implementation.
- ✧ Get alerted in real time on sensitive data being added to workspaces.
- ✧ Detects Personally Identifiable Information as well.
- ✧ Chrome Extension to test your site post deployment.
- ✧ Revoke access to your data instantly
- ✧ Check public search engines for leaks
- ✧ Automate revoking rules
- ✧ 100% On-Device Scanning, No data stored

# ✦ COMPONENTS OF THE ARCHITECTURE ✦



## EXECUTABLE

The main engine and heart of the project which runs locally on your system



## EXTENSION

The Chrome extension to perform tests on the browser post-deployment



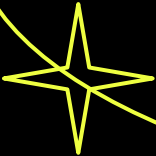
## INTERFACE

Visual Interface to Handle Outputs to the user and grab inputs



**01**

**CORE  
EXECUTABLE**

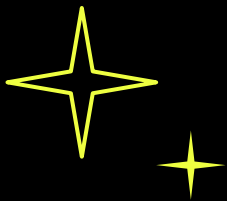




# CORE EXECUTABLE



This component is indispensable for maintaining proactive security measures throughout the software development lifecycle. By continuously monitoring local machines, it can promptly detect any accidental leaks of sensitive information like authentication tokens and API keys. This proactive approach ensures that potential vulnerabilities are identified early on, allowing developers to take corrective action before deployment. The active scanning script not only enhances the security posture of the project but also instills confidence in stakeholders regarding the protection of valuable assets.



# 02

## CHROME EXTENSION





# CHROME EXTENSION

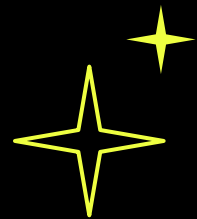


The Chrome extension serves as a vital tool for developers by providing an additional layer of security during the code review process. It analyzes the source code for any exposed secrets, such as private cryptographic keys, thereby mitigating the risk of unintentional information disclosure. This component seamlessly integrates into the development workflow, enabling developers to identify and address security issues directly within their preferred browser environment. With the Chrome extension's assistance, developers can maintain code integrity and uphold security best practices while streamlining their development workflow.



03

# USER INTERFACE





# CHROME EXTENSION



The Chrome extension serves as a vital tool for developers by providing an additional layer of security during the code review process. It analyzes the source code for any exposed secrets, such as private cryptographic keys, thereby mitigating the risk of unintentional information disclosure. This component seamlessly integrates into the development workflow, enabling developers to identify and address security issues directly within their preferred browser environment. With the Chrome extension's assistance, developers can maintain code integrity and uphold security best practices while streamlining their development workflow.

# Reducing False Positives:

Leveraging CVSS and EPSS

Ratings

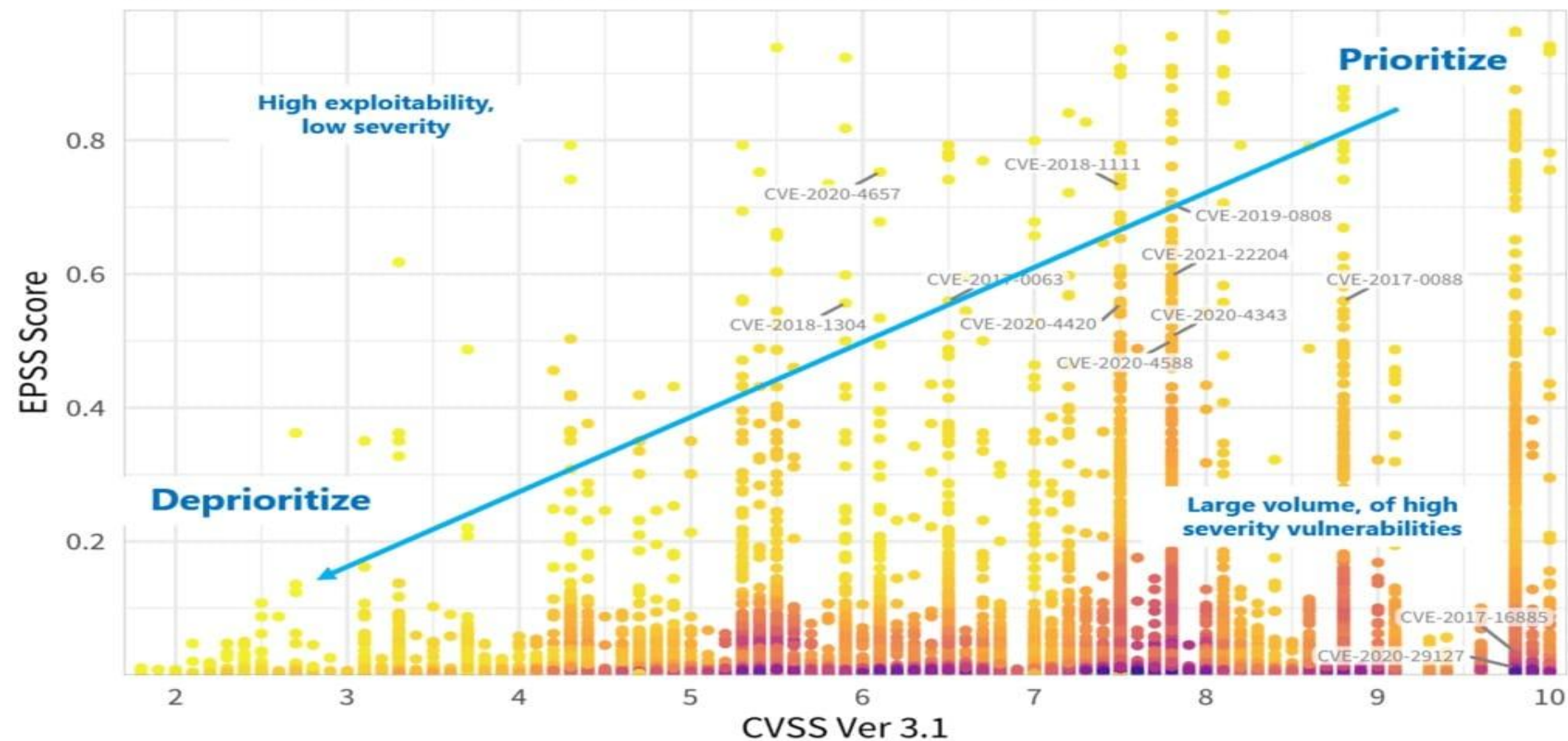
# ✦ Reducing False Positives ✦

False positives were a significant challenge in our security scanning tool, often leading to wasted time and resources as users sift through irrelevant alerts. To address this issue effectively, we employed a sophisticated approach that leverages Common Vulnerability Scoring System (CVSS) and Enhanced Prioritization of Security Signals (EPSS) ratings.

This section explores how these ratings are generated and utilized to analyze the usefulness of data, thereby reducing false positives.

## EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.

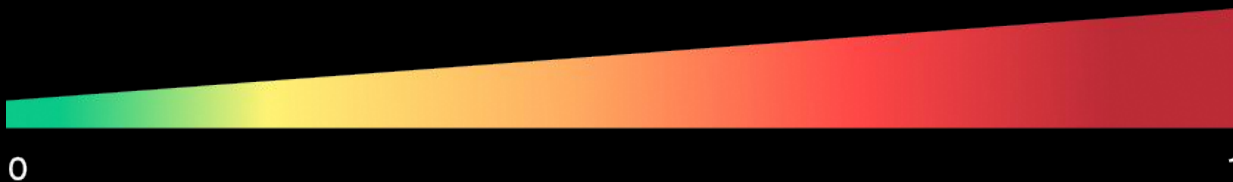




# WHAT IS EPSS?



Exploit Prediction Scoring System is a data-driven approach to assessing the likelihood of a software vulnerability being exploited. By leveraging data from past exploits, threat intelligence feeds, and system configurations, EPSS calculates a comprehensive score indicating the probability of an exploit occurring.



Scoring Range: 0 to 1



# HOW DOES THIS HELP?



## PRIORITISING

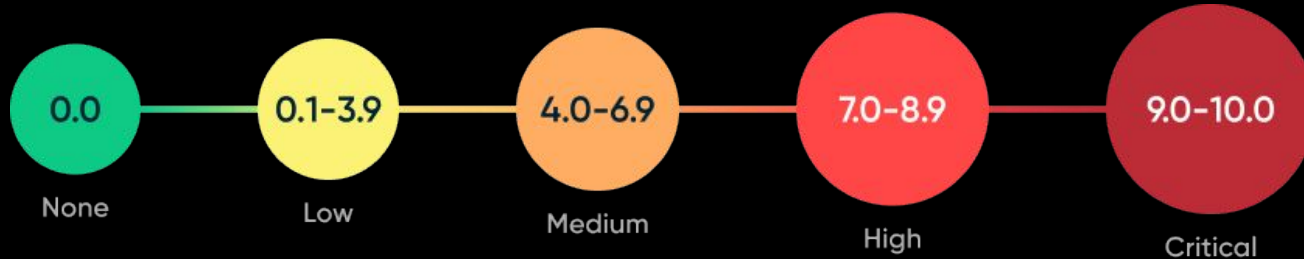
Prioritize vulnerability remediation efforts and focus on the most pressing threats.

## ESTIMATING

Probability of an attack happening in the coming 30 days or so.

# WHAT IS CVSS?

Common Vulnerability Scoring System for assessing the severity of cybersecurity vulnerabilities. It offers a structured framework that considers various aspects of a vulnerability impact and exploitability to generate a numerical score.



Scoring Range: 0 to 10



# SCORE FACTORS





# CVSS 4.0: WHAT'S NEW?



## Base Metric Group

### EXPLOITABILITY METRICS

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Attack Requirements

### IMPACT METRICS

- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

## Threat Metric Group

- Exploit Code Maturity

## Supplemental Metric Group

- Automatable
- Recovery
- Safety
- Value Density
- Vulnerability Response Effort
- Provider Urgency



# CVSS 4.0: WHAT'S NEW?



## Environmental Metric Group



Confidential  
Requirement



Availability  
Requirement



Integrity  
Requirement



Modified Base Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction
- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

Key:



Existing Component from CVSS 3.1

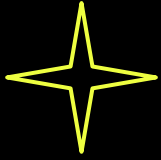


Existing Component with Substantial Change



New CVSS 4.0 Component

Source: [www.first.org](http://www.first.org)



# THANK YOU

And welcome to the future of privacy :)

