

# **Sri Lanka Institute of Information Technology**



**IE2012 - System and Network Programming**

**Bug Bounty Progress Submission**

**Name: De Silva K.R.K.D**

**Student ID: IT22151056**

**Submission Date: 2023/09/13**

# Introduction

My goal is to improve my cybersecurity skills to help make the digital world more safe. Every challenge I overcame during this journey taught me more about online security. I developed my problem-solving abilities and learned how to recognize and respond to potential security issues through a process of ongoing learning. On websites like PortSwigger, OvertheWire, and PicoCTF web security academy, I faced a variety of difficulties. These difficulties forced me to step outside of my comfort zone and gave me the knowledge and talents to accurately identify and communicate vulnerabilities. I gained knowledge of cybersecurity principles along the road.

# Progress Overview:

My main objective throughout my bug bounty journey has been to improve my cybersecurity capabilities with the ultimate goal of making the internet a safer place. Every obstacle I met along the way provided me with a priceless lesson in online security, greatly enhancing my knowledge of the subject. As I overcame these difficulties, I improved not only my problem-solving skills but also my capacity to spot risks. Continuous learning has characterized this journey, highlighting the notion that cybersecurity is a field that is constantly changing.

## **Bug bounty programs I participated in**

**Natas:** <https://overthewire.org/wargames/natas/>

- My Natas report: [https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056\\_my\\_sliit\\_lk/Ec7zHiqbdBpHiDnuu1bf6yoBlZgv-Tl3qQhfTGPegoBjKw?e=GRkRp6](https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056_my_sliit_lk/Ec7zHiqbdBpHiDnuu1bf6yoBlZgv-Tl3qQhfTGPegoBjKw?e=GRkRp6)

Natas is interactive by OverTheWire to instruct and assess knowledge of web security and ethical hacking. Players are given a number of levels in Natas, each of which has a unique set of website vulnerability-related difficulties. As players advance over the levels, a variety of security vulnerabilities will come up, from simple configuration errors to more advanced exploitation strategies. The foundations of server-side web security are taught by Natas. Each level has its own website. SSH login is not available for this one. Natas

offers a practical learning platform for people wishing to develop their web security expertise in a useful and entertaining manner.

The screenshot shows the OverTheWire Natas wargame page in a web browser. The browser's address bar displays <https://overthewire.org/wargames/natas/>. The page has a dark theme. At the top, there's a navigation bar with 'Wargames' and 'Information' links, and the 'OverTheWire' logo with the tagline 'We're hackers, and we are good-looking. We are the 1%.' To the right of the logo are 'Donate!' and 'Help!?' buttons. Below the navigation bar, the page is titled 'Natas'. On the left side, there's a vertical list of levels from 'Level 0' to 'Level 31', each followed by an arrow pointing to the next level. The main content area starts with 'Level 0' and describes the basics of serverside web-security. It explains that each level has its own website at <http://natasX.natas.labs.overthewire.org>, where X is the level number. It notes that there is no SSH login and provides instructions on how to access a level using a username and password. It also mentions that passwords are stored in `/etc/natas_webpass/`. A 'Start here:' section provides the following details:  
Username: `natas0`  
Password: `natas0`  
URL: `http://natas0.natas.labs.overthewire.org`  
On the right side of the main content area, there is a logo for 'NESSoS' and a note stating 'developed in association with the NESSoS FP7 project'.

## Bandit:

<https://overthewire.org/wargames/bandit/>


- My Bandit report: [https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056\\_my\\_sliit\\_lk/EUY6MEZmgD5Njxx7u-Zb2SsBHmdKKMzvvlgnHl7fiHu01A?e=xywqeU](https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056_my_sliit_lk/EUY6MEZmgD5Njxx7u-Zb2SsBHmdKKMzvvlgnHl7fiHu01A?e=xywqeU)

OverTheWire created the Linux virtual computer known as Bandit, which is purposefully insecure. It provides a useful platform for people who want to improve their command-line and ethical hacking. Bandit has several levels, each of which presents its own special set of security-related difficulties. Users come across missions in order to go through the levels that call for them to use various Linux commands and strategies, locate passwords, and attack system vulnerabilities. Bandit provides a hands-on and real-world learning environment, making it the perfect place to start for people interested in learning about OS security.

← → ↺

🔒 <https://overthewire.org/wargames/bandit/>

📄 ☆ 📧 ⬇️ 🔧 📁 🚫 ☰



Wargames updated Information

OverTheWire  
We're hackers, and we are good-looking. We are the 1%.

Donate! Help?

SSH Information  
Host: bandit.labs.overthewire.org  
Port: 2220

Bandit

Level 0 → Level 1  
Level 1 → Level 2  
Level 2 → Level 3  
Level 3 → Level 4  
Level 4 → Level 5  
Level 5 → Level 6  
Level 6 → Level 7  
Level 7 → Level 8  
Level 8 → Level 9  
Level 9 → Level 10  
Level 10 → Level 11  
Level 11 → Level 12  
Level 12 → Level 13  
Level 13 → Level 14  
Level 14 → Level 15  
Level 15 → Level 16  
Level 16 → Level 17  
Level 17 → Level 18  
Level 18 → Level 19  
Level 19 → Level 20  
Level 20 → Level 21  
Level 21 → Level 22  
Level 22 → Level 23  
Level 23 → Level 24  
Level 24 → Level 25  
Level 25 → Level 26  
Level 26 → Level 27  
Level 27 → Level 28  
Level 28 → Level 29  
Level 29 → Level 30

## Bandit

The Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. **If you notice something essential is missing or have ideas for new levels, please let us know!**

### Note for beginners

This game, like most other games, is organised in levels. You start at Level 0 and try to "beat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level <X>" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the sidemenu on the left of this page.

You will encounter many situations in which you have no idea what you are supposed to do. **Don't panic! Don't give up!** The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information. If you've never used the command line before, a good first read is [this introduction to user commands](#).

There are several things you can try when you are unsure how to continue:

First, if you know a command, but don't know how to use it, try the **manual** (man page) by entering **man <command>**. For example, **man ls** to learn about the "ls" command. The "man" command also has a manual, try it! When using **man**, press q to quit (you can also use / and n and N to search).

Second, if there is no man page, the command might be a **shell built-in**. In that case use the **"help <X>"** command. E.g. **help cd**

Also, your favorite **search-engine** is your friend. Learn how to use it! I recommend Google.

Lastly, if you are still stuck, you can [join us via chat](#)

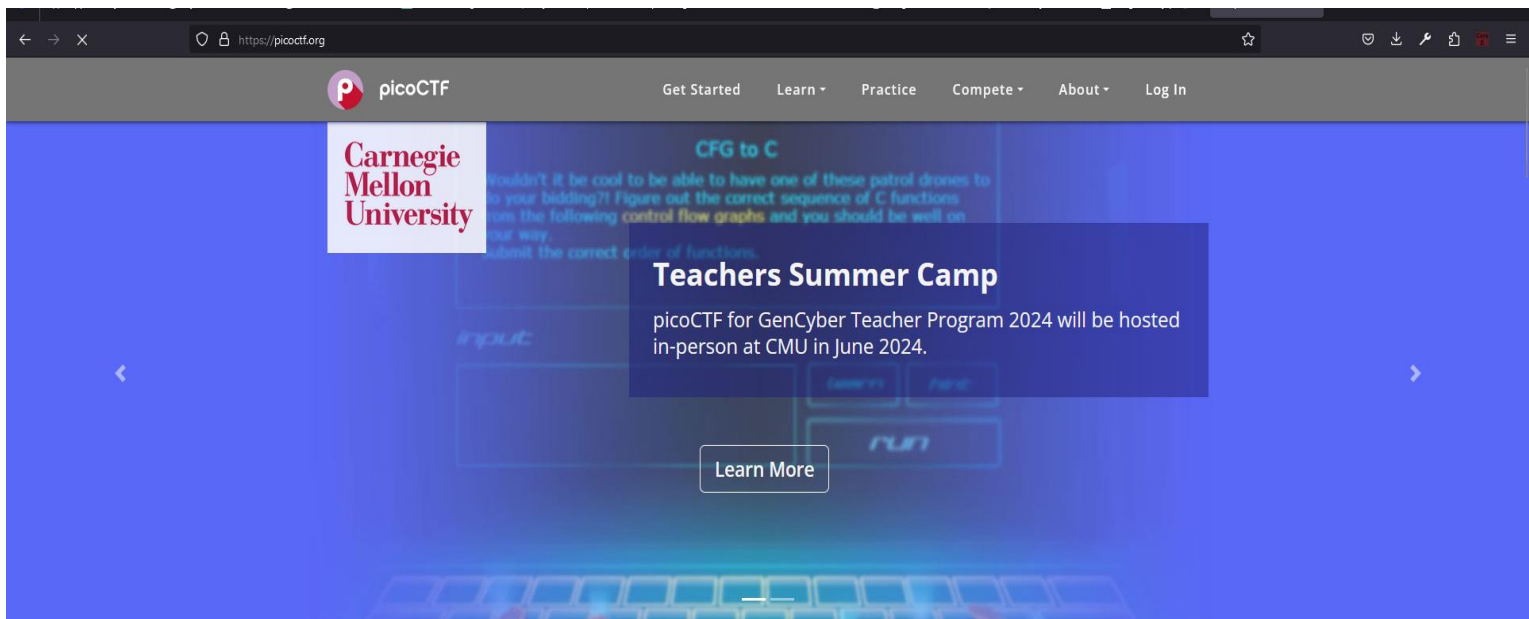
You're ready to start! Begin with Level 0, linked at the left of this page. Good luck!

**Note for VMs:** You may fail to connect to overthewire.org via SSH with a *"broken pipe error"* when the network adapter for the VM is configured to use NAT mode. Adding the setting **IPQoS throughput** to `/etc/ssh/ssh_config` should resolve the issue. If this does not solve your issue, the only option then is to change the adapter to Bridged mode.

**PicoCTF:** <https://picoctf.org/>

- My Bandit report: [https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056\\_my\\_sliit\\_lk/EaP6RxCY589Ps3\\_dmqc20HkBuy7ZneFtlGLQFlbKJ\\_gqUA?e=HEVrIN](https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056_my_sliit_lk/EaP6RxCY589Ps3_dmqc20HkBuy7ZneFtlGLQFlbKJ_gqUA?e=HEVrIN)

The goal of is to educate and challenge people in the field of cybersecurity through an online platform and capture the flag tournament. The platform offers an organized and interactive environment to learn and apply cybersecurity skills, and is used by both novice and expert hackers. For individuals curious about the field of cybersecurity and ethical hacking, PicoCTF offers an entertaining and informative experience, whether it's time to test the knowledge or improve skills.



## picoCTF is for everyone



picoCTF gamifies learning hacking with capture-the-flag puzzles created by trusted computer security and privacy experts at [Carnegie Mellon University](https://www.cmu.edu).

**PotrSwigger:** <https://portswigger.net/>

- My PortSwigger report: [https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056\\_my\\_sliit\\_lk/ES1buoHpKKZApdU0wYgiZkYBPhTfyfCNeHVOPDg1PluWww?e=AMATA5](https://mysliit-my.sharepoint.com/:b:/g/personal/it22151056_my_sliit_lk/ES1buoHpKKZApdU0wYgiZkYBPhTfyfCNeHVOPDg1PluWww?e=AMATA5)

One of the leading names in web application security testing and investigation is PortSwigger. They specialize in locating and fixing serious bugs like SQL injection and XXE. Attackers can alter XML input thanks to the XXE vulnerability, which could result in data breaches or server penetration. On the other side, a vulnerability known as SQL injection can allow hackers to enter a database without authorization and retrieve, edit, or destroy sensitive data. The tools and resources provided by PortSwigger enable companies to protect themselves against these and other security risks, making the internet a safer place for everyone.

The screenshot shows the PortSwigger website with a navigation bar including 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main content area features the text 'Secure your world.' and 'PortSwigger products help more than 70,000 professionals - at over 16,000 organizations - to secure the web and speed up software delivery.' Below this is a 'FIND OUT MORE' button. To the right, a man is shown working on a laptop, with a large, semi-transparent image of the Burp Suite interface overlaid. The interface displays 'Current issues' with a donut chart showing 303 total issues (High: 75, Medium: 9, Low: 20, Information: 198). It also shows 'Most serious vulnerabilities' with a list of issues like 'Serialized object in HTTP message' and 'Flash cross-domain policy'. The bottom of the page features three accolades: 'Gartner peer insights customers' choice', 'Best in class for security testing', and 'A must-have tool for security engineers'.

**PortSwigger**

Secure your world.

PortSwigger products help more than 70,000 professionals - at over 16,000 organizations - to secure the web and speed up software delivery.

**Burp Suite**

Current issues: 303

Most serious vulnerabilities:

- Serialized object in HTTP message
- Flash cross-domain policy
- Cross-site scripting (DOM-based)
- Cross-site scripting (reflected)

"Best in class for security testing"

"A must-have tool for security engineers"

# **Bug Bounty**

A bug bounty program is a preventive cybersecurity campaign in which businesses pay ethical hackers, often known as white hat hackers, to find bugs in their computer system, such as software or websites. . A variety of organizations, and programmers provide bug bounty programs as a way for people to be rewarded and paid for reporting bugs, particularly those that relate to security exploits and vulnerabilities.

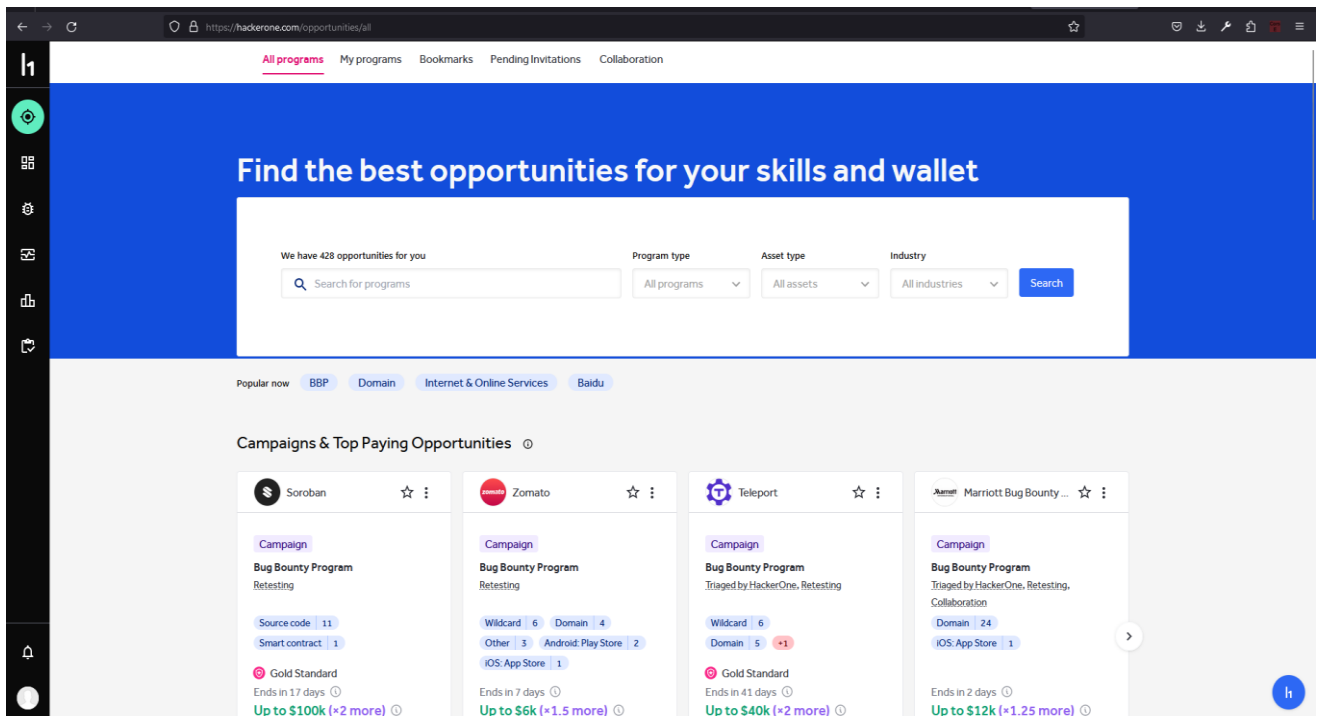
The hackers receive financial awards, joy, or additional rewards in return for correctly exposing these flaws business in finding and fixing security flaws before criminal hackers can take advantage of them, eventually improving the overall safety and durability of digital systems. This collaborative approach has grown in popularity as an essential element in modern cybersecurity tactics, ensuring that bugs are quickly identified and fixed to safeguard sensitive data and preserve user and consumer trust.

## **Targeted Websites**

### **HackerOne**

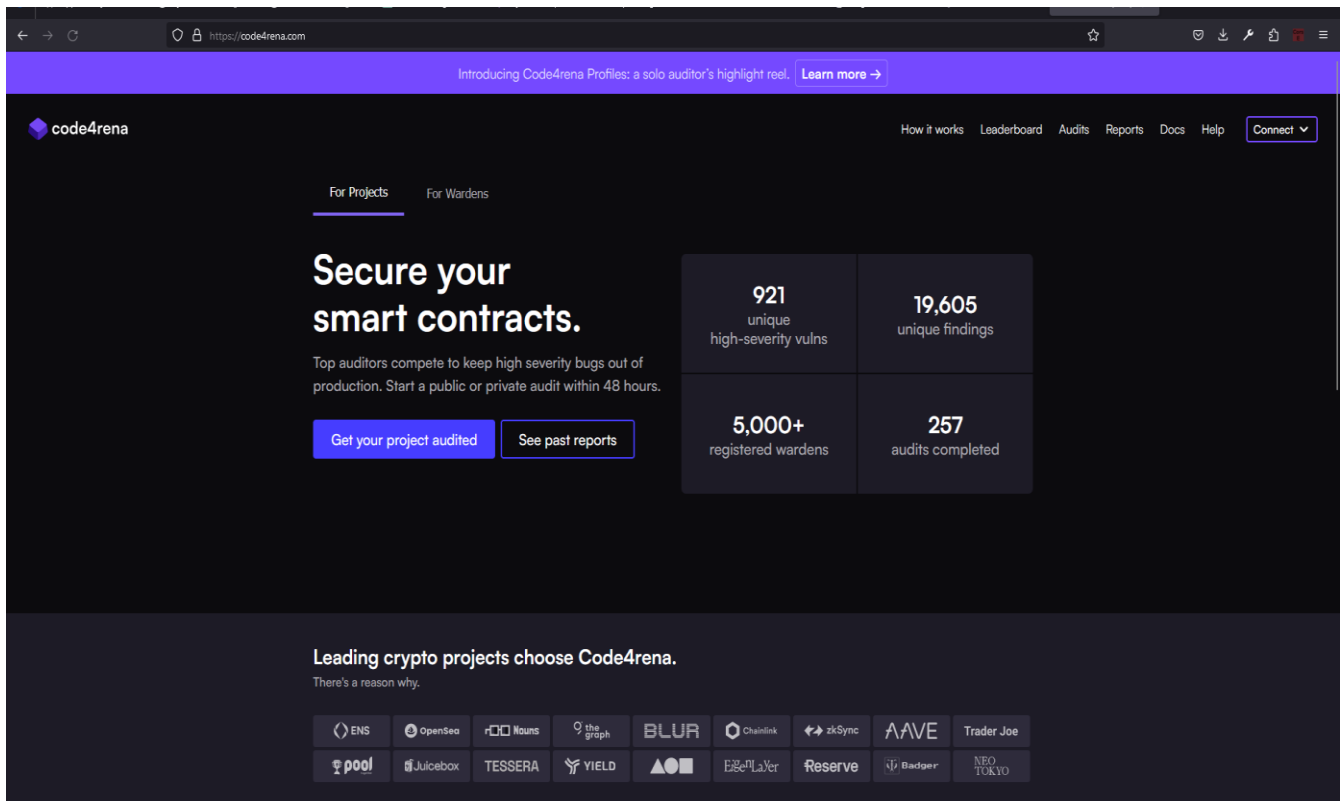
In the fields of ethical hacking and vulnerability release, HackerOne is top platform. HackerOne was created as a link between businesses and ethical hackers, facilitating bug-bounty schemes and vulnerability coordinating services. With their website, they link businesses looking to find and fix security issues in their digital assets with knowledgeable security researchers from across the world. In order to create an integrated approach to cybersecurity, HackerOne has established itself as a reliable partner for corporations and government organizations. Hackerone helps businesses strengthen their defenses and safeguard sensitive data by offering a secure and organized setting for hackers to disclose vulnerabilities.





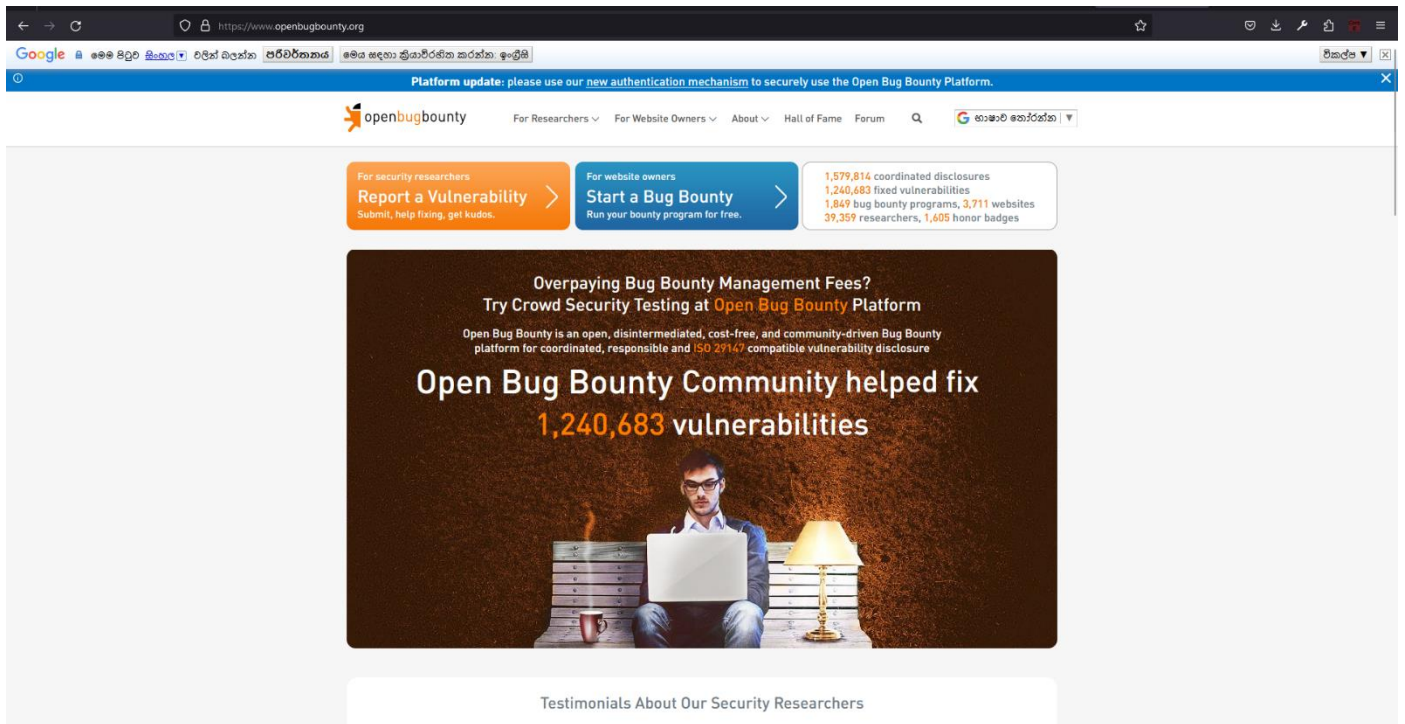
## Code4rena

Software engineers and coders can compete in coding challenges on the interesting and cutting-edge Code4rena platform. Programmers from all around the world may demonstrate their abilities, work together to solve challenging challenges, and obtain rewards in this dynamic and exciting environment. Coding enthusiasts can take part in a selection of coding competitions and contests at Code4rena, ranging in complexity and scope. These tasks include a wide range of codes and ideas, giving developers a great chance to broaden their knowledge and skills.



## Yes We Hack

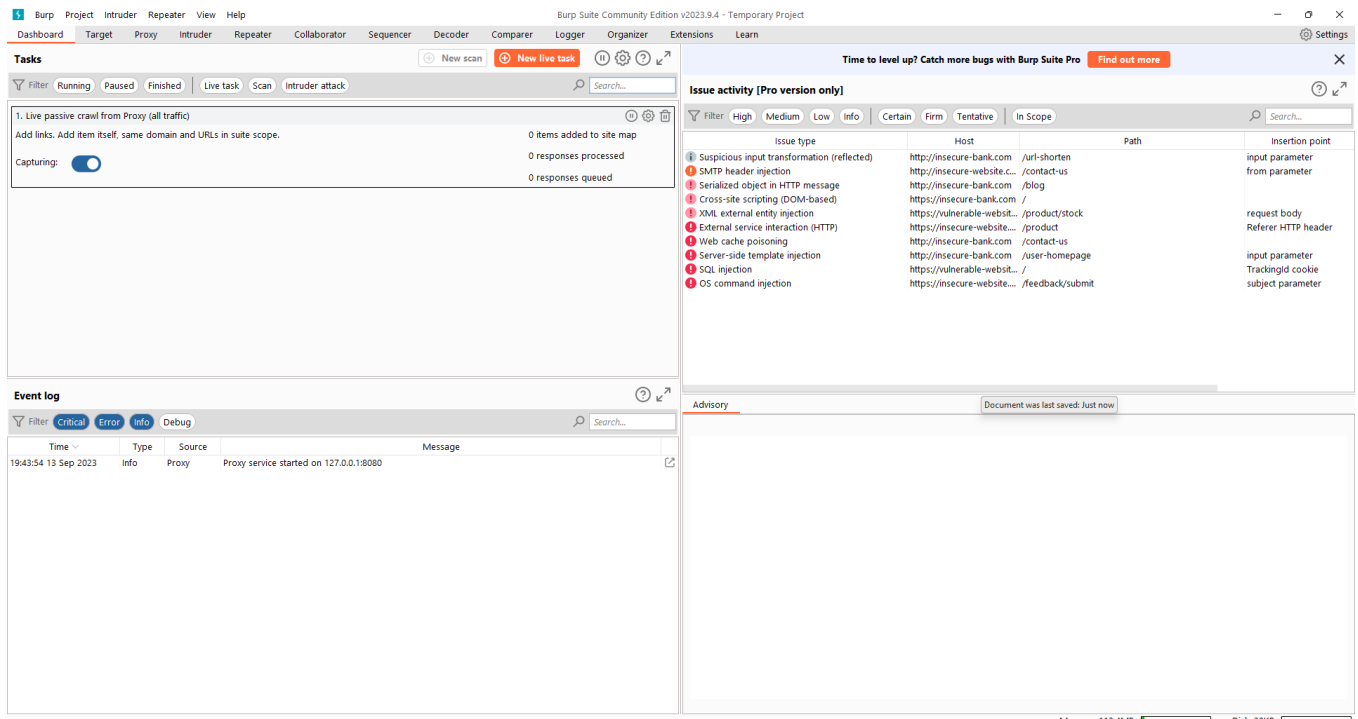
A modern cybersecurity platform called “Yes We Hack” acts as a link between businesses looking to improve their online security and a large community of knowledgeable ethical hackers. Utilizing their knowledge to find and fix vulnerabilities before criminal actors can take advantage of them, corporations, government organizations, and institutions may tap into a sizable talent pool of cybersecurity professionals thanks to this ground-breaking platform. With a focus on ethical hacking, and preventative safeguards, “Yes We Hack” offers a safe and effective solution to improve digital security, guaranteeing that your digital possessions are protected in a world that is becoming more interconnected.



## Bug-bounty tools

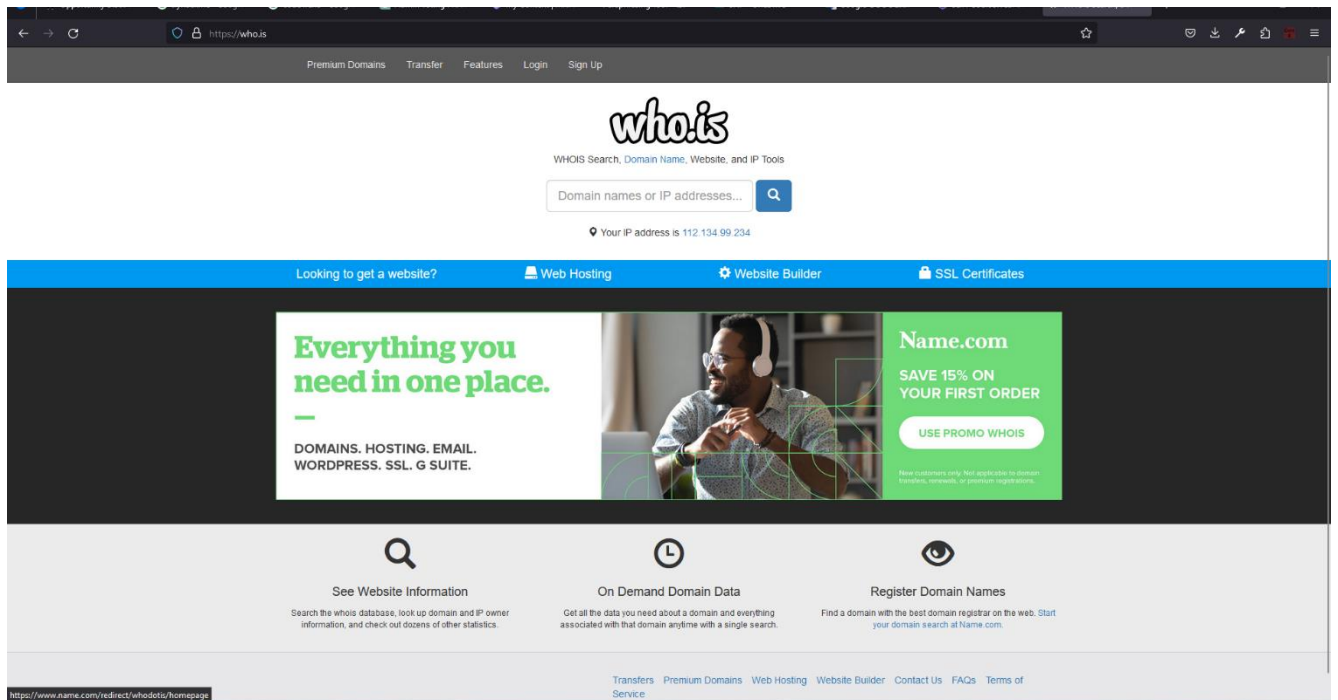
### Burp Suite

Burp Suite is a robust and well-liked cybersecurity tool made for testing and evaluating web application security. It was created by PortSwigger and is a vital tool for security experts, responsible hackers, and developers to find and fix vulnerabilities in web applications. Burp Suite is an essential tool for anyone concerned with protecting web applications from threats and guaranteeing its durability due to its extensive feature set, which includes web vulnerability assessment, proxy interception, and detailed reporting.



## who.is

A useful web resource that offers details on domains and their owners is who.is. It functions as an open database where you can search up specifics about a domain, including its registration and expiration dates as well as the owner, administrator, and registrar's contact information. People, companies, and cybersecurity experts routinely utilize who.is for a variety of reasons, such domain research, legal questions, and spotting possible problems with internet domains. It is an essential tool for learning about the ownership and background of internet domains.



## Nmap

The advanced open-source network scanning and spying application Nmap is available for free. Nmap is used to find and evaluate devices and services within computer networks by cybersecurity experts, network administrators, and ethical hackers. It is widely considered as a norm for system exploration and security auditing. To give helpful insights into the network's layout, port availability, service form, and potential vulnerabilities, it makes use of a range of scanning techniques. Nmap is an essential instrument to use for offensive and defensive network security strategies, assisting in both the assessment of security positions and the identification and correction of configuration flaws in networks.

← →

https://nmap.org


☆

📄

🔍

🔒

☰



NEW Search

🔍

Download

Reference Guide

Book

Docs

Zenmap GUI

In the Movies

Get Nmap 7.94 here

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on [Npcap.com](#), [Seclists.org](#), [Insecure.org](#), and [SecTools.org](#).
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [\[Release Announcement\]](#) [\[Download page\]](#)
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [\[Release Announcement\]](#) [\[Download page\]](#)
- Nmap 7.80 was released for DEFCON 27! [\[release notes\]](#) [\[download\]](#)
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading [the original Phrack #51 article "Nmap20!"](#)
- Nmap 7.50 is now available! [\[release notes\]](#) [\[download\]](#)
- Nmap 7 is now available! [\[release notes\]](#) [\[download\]](#)
- We're pleased to release our new and improved [Icons of the Web](#) project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also to [launch nuclear missiles in G.I. Joe: Retaliation!](#)
- We're delighted to announce Nmap 6.40 with 14 new [NSE scripts](#), hundreds of new [OS](#) and [version detection](#) signatures, and many great new features! [\[Announcement Details\]](#) [\[Download Site\]](#)
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [\[Announcement Details\]](#) [\[Download Site\]](#)
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with [Nmap 6.01!](#)
- Nmap 6 is now available! [\[release notes\]](#) [\[download\]](#)
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of like Yelp for security tools. Are you familiar with all of the [49 new tools](#) in this edition?
- [Nmap 5.50 Release!](#) Now with Coepher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,962 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [\[Download page\]](#) [\[Release notes\]](#)
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam—all in 38 minutes! [\(Presentation video\)](#)
- [Icons of the Web](#): explore favicons for the top million web sites with our [new poster and online viewer](#).
- We're delighted to announce the immediate, free availability of the [Nmap Security Scanner version 5.00](#). Don't miss the [top 5 improvements](#) in Nmap 5.
- After years of effort, we are delighted to release [Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!](#)
- We now have an active Nmap [Facebook page](#) and [Twitter feed](#) to augment the [mailing lists](#). All of these options offer RSS feeds as well.

Nmap: Discover your network