Ghidra Collaborative Reversing 1/2 — How to setup a Ghidra server

Jannis Kirschner Follow
Mar 14 · 4 min read

Introduction

Ghidra Server allows multiple reverse engineer to share a project and work together, similar to the IDArling plugin for Ida Pro (https://github.com/IDArlingTeam/IDArling). Ghidra Server gets shipped by default and can be installed on Windows, Linux and Mac OS.

Overview over installation steps

- First you need to download Ghidra
- Then you need to edit the server.conf file
- Afterwards you can install the service
- Finally you can add users and repositories

Files (.\ghidra_9.0\server)

- “ghidraSvr.bat” — Start/stop the ghidra server, shows status of server
- “svrAdmin.bat” — Add/remove users, manage repositories
- “svrInstall.bat” — Installs the service
- “svrUninstall.bat” — Removes the service
- “server.conf” — Configuration file

User Management

Ghidra supports multiple means of authentication.

- (-a0) Local Ghidra Password. Default is changeme. Passwort is stored hashed in .\repository\users
- (-a1) Native OS Password. Windows only and broken in newer windows versions!
- (-a2) PKI authentication. Authentication over certificates.
- (-a3) Native OS PW+ Local Ghidra PW. Broken aswell!

- (-ssh) SSH public key file. Only limited functionality.

Reference for issues:
https://github.com/NationalSecurityAgency/ghidra/issues/167

Step-by-Step Installation

We will setup a server with the “Local Ghidra Password” option on a Windows Server 2012 R2.

Step 1: Download Ghidra

GHIDRA Webpage

- Goto: https://ghidra-sre.org/
- Download the zip file
- Unzip it to your preferable installation directory
- Create an empty directory on a different location to store the repository

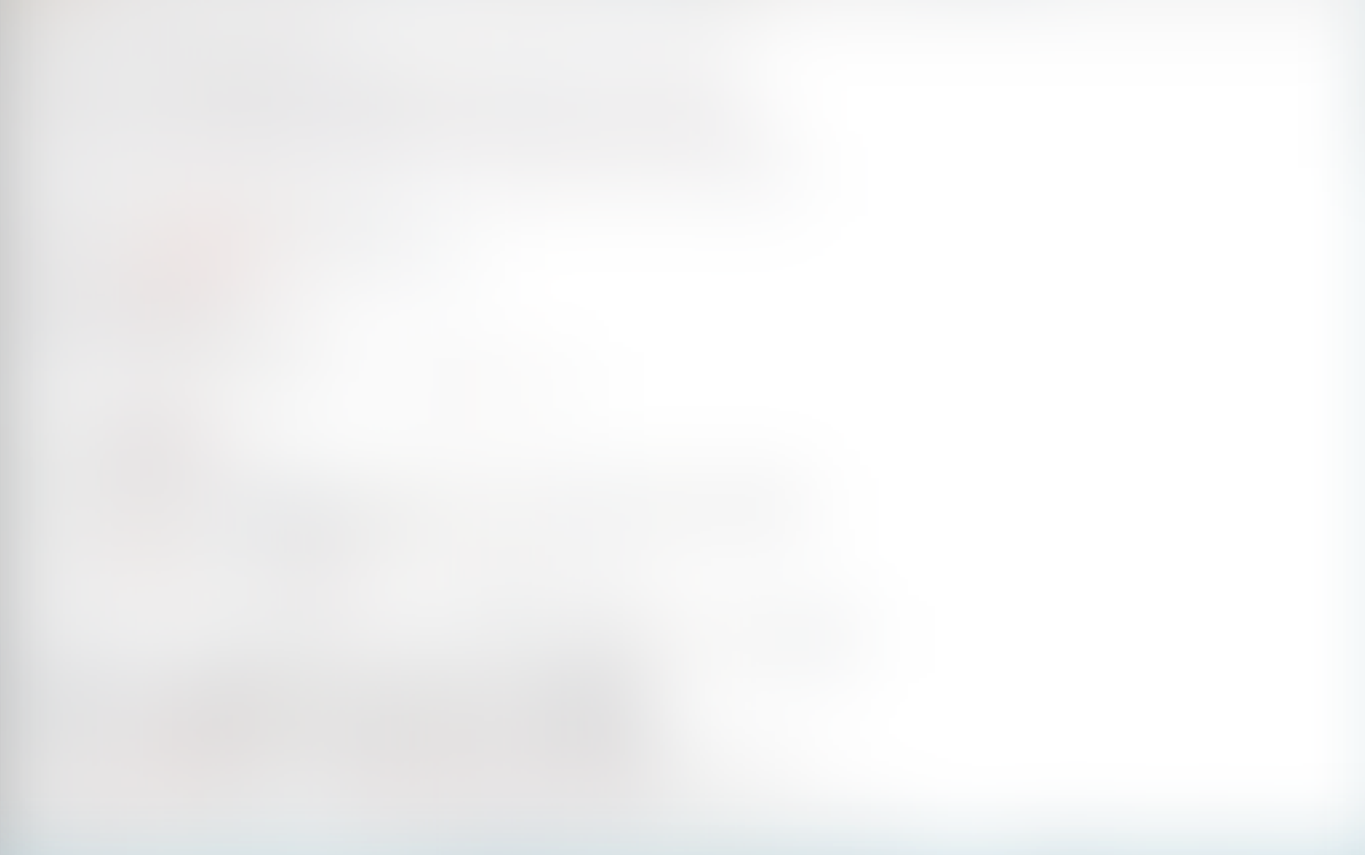
Step 2: Download Java

- You need to download the jdk 11 for ghidra to run.
  Get it from here:
  https://www.oracle.com/technetwork/java/javase/downloads/jdk11-downloads-5066655.html

- After downloading, run it and follow the installation instructions

JDK Downloadpage

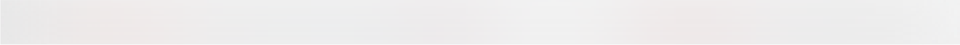
Step 3: Edit Configuration



Ghidra Server Configuration File

Open .\ghidra_9.0\server\server.conf in your favorite text editor. Change the following lines:

- Change “ghidra.repositories.dir” to your newly created directory



- Add some parameters to Line 125+ (user changeable and predefined ip interface)

Step 4: Test and service installation

- Open a root shell and navigate to your server directory
- Run ghidraSvr.bat (If you get a windows firewall request, accept it)

Testwise running a ghidra server instance

If you can start it without any errors you can close the window and install the service by running the “svrInstall.bat” script.

Installing the ghidra server service

Afterwards you can verify it by running ghidraSvr.bat with the status argument:

Getting the status of ghidra server

You can now start/stop the server with the ghidraSvr.bat script and the arguments “start”/”stop”.

Starting the ghidra server service

Step 5: Add users

- Make sure the server is stopped and not running.
- Now you can use the “svrAdmin.bat” script to add a user.

The README defines to pass an SID which can be kinda misleading. You simply need to pass a username not a Windows Secure Identifier.

Step 6: Finalize

- Afterwards you can start the service.
- Then you can start Ghidra and open “File” -> “New Project”.

Connect to the IP-Address or DNS-Name of your server.

Connecting to the server from the ghidra client

Your default password is “changeme”.

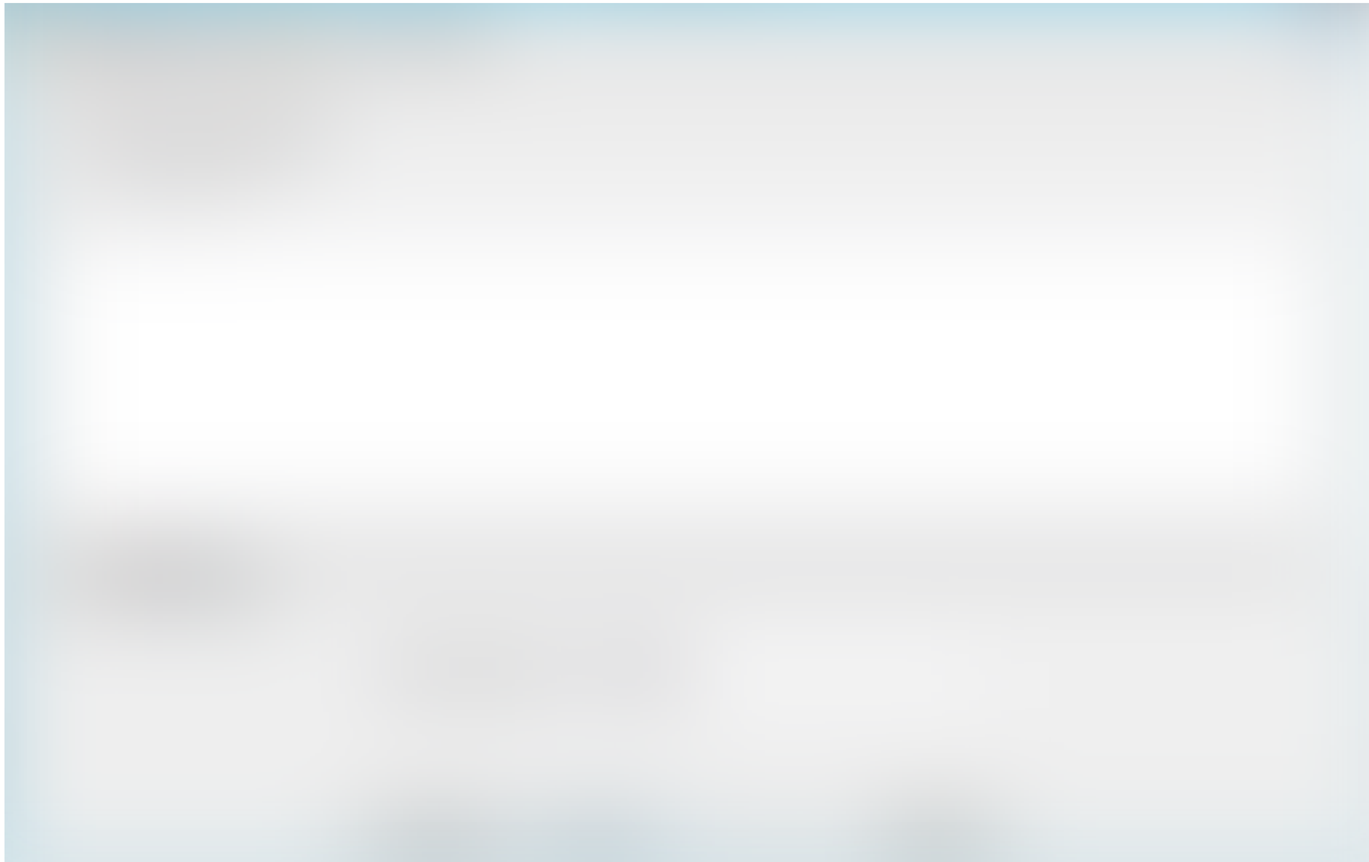
Authentication with default password

You can always reset it to “changeme” with “svrAdmin.bat -reset <username>”.

After the first login you are being prompted to reset the password.

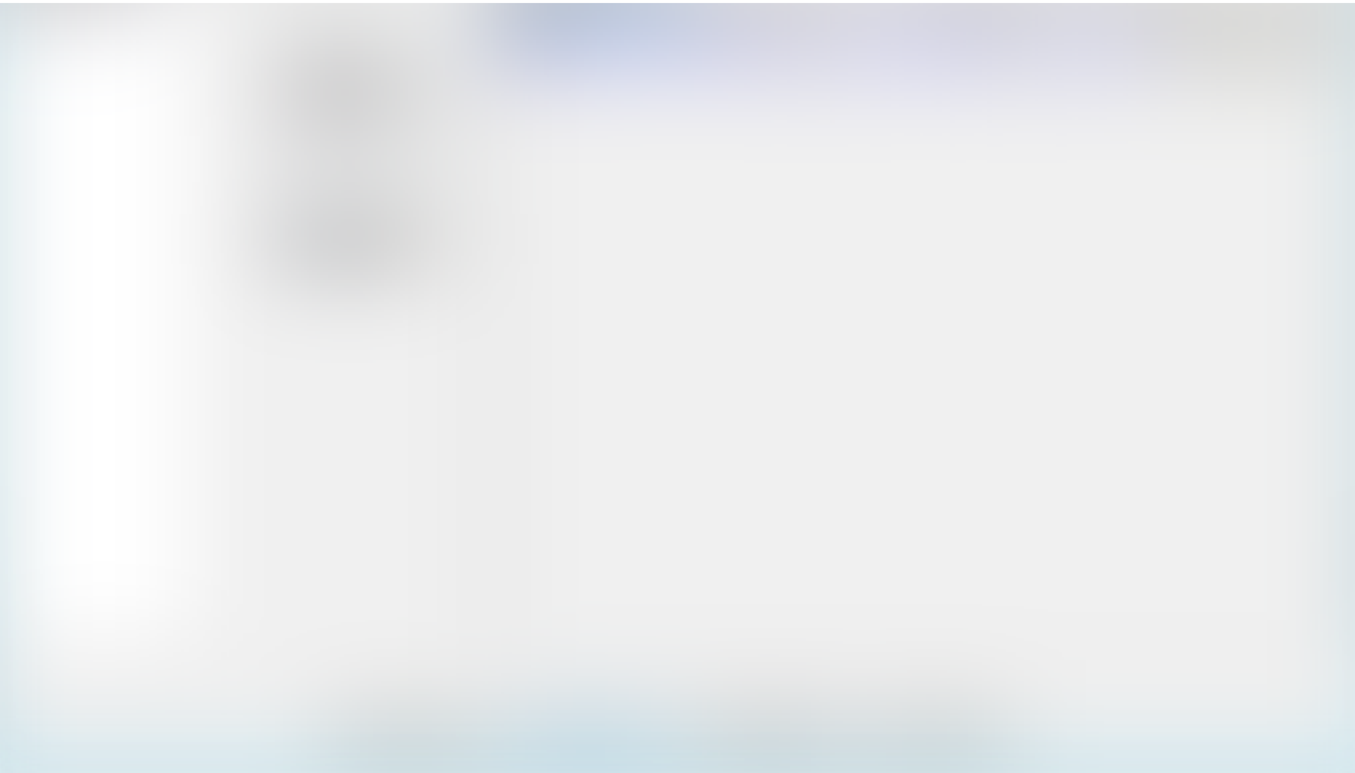
Mandatory password change

Now you can create a new repository.



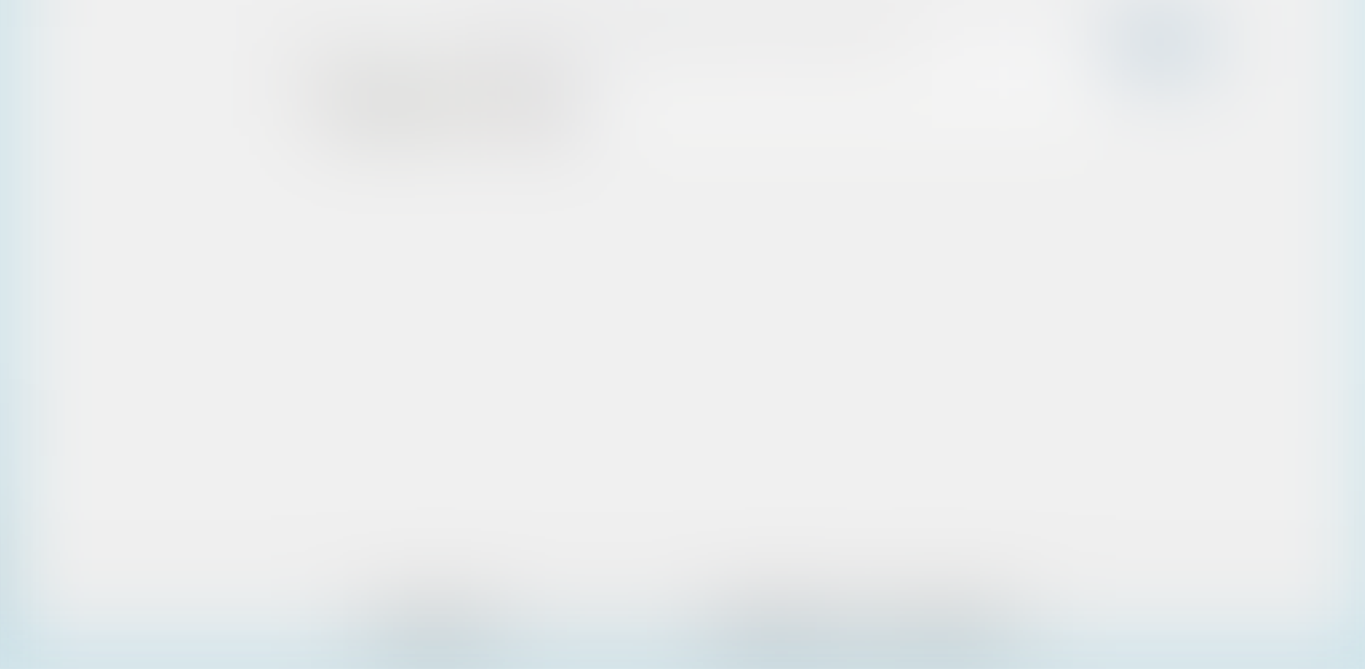
Creating a new ghidra project

And set permissions for your users.



Setting project permissions

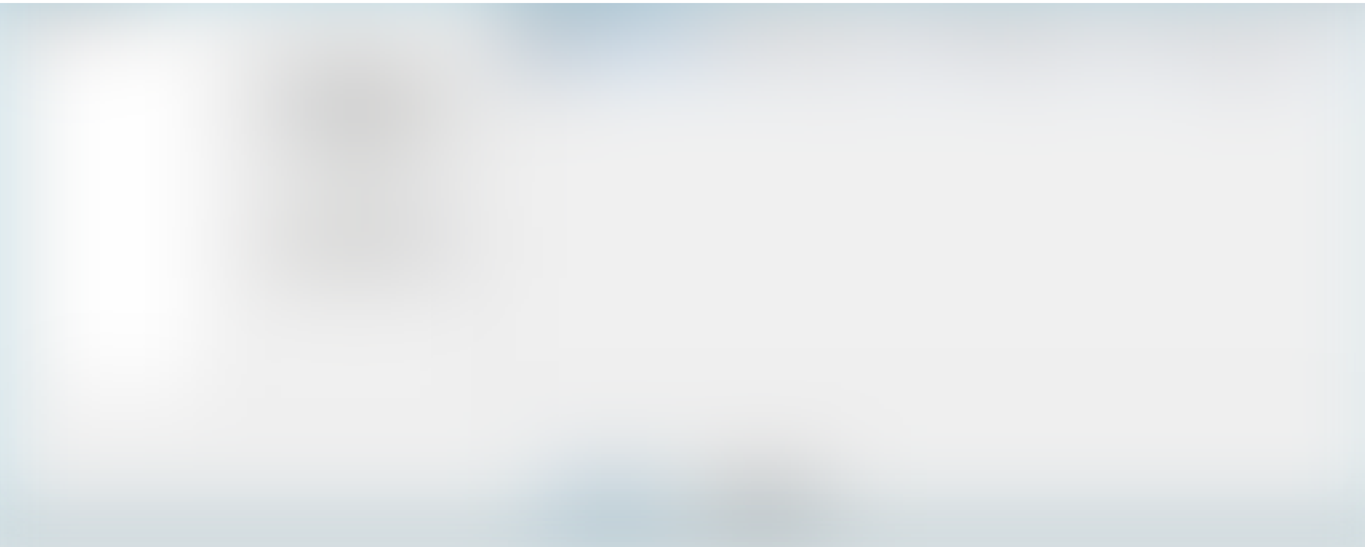
Finally choose a path for your local project files.



Choosing a local repository path

Changing Permissions:

If you need to adjust permissions after setup of a repository you can add them with “svrAdmin.bat”. Afterwards in Ghidra you can open the project with an admin account and go to “Project” -> “Edit Project Access List”



Changing the ACL for a project

. . .

Summary

In this tutorial we have set up a ghidra server for collaborative reverse engineering. In the next part we are going to have a look at some of the features of the ghidra server.

Thank you for reading :)

Ghidra · Reverse Engineering · Cybersecurity · Malware Analysis · Hacking

51 claps

WRITTEN BY

Jannis Kirschner

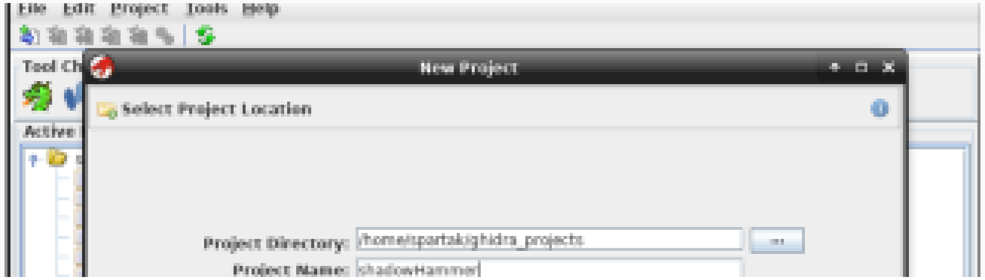
Follow

Swiss Security Researcher & CTF Enthusiast

Write the first response

More From Medium

Also tagged Ghidra



Project Directory: /home/spartak/ghidra_projects

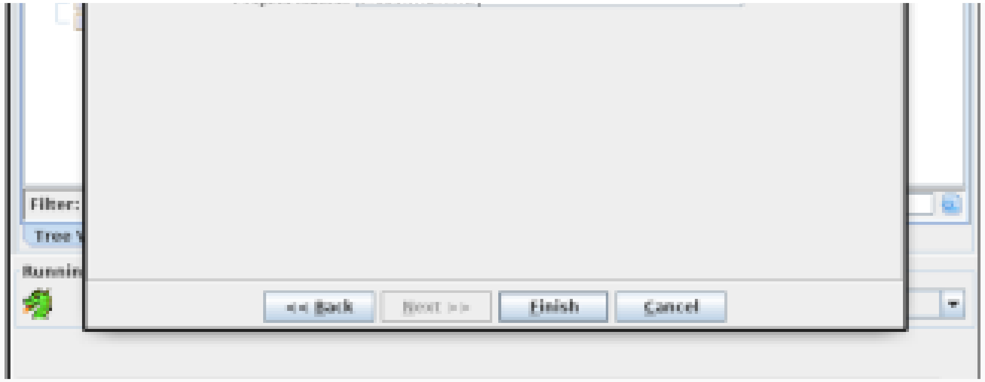
Project Name: ShadowHammer

Practice with Ghidra

nowayout

May 5 · 5 min read ★

49



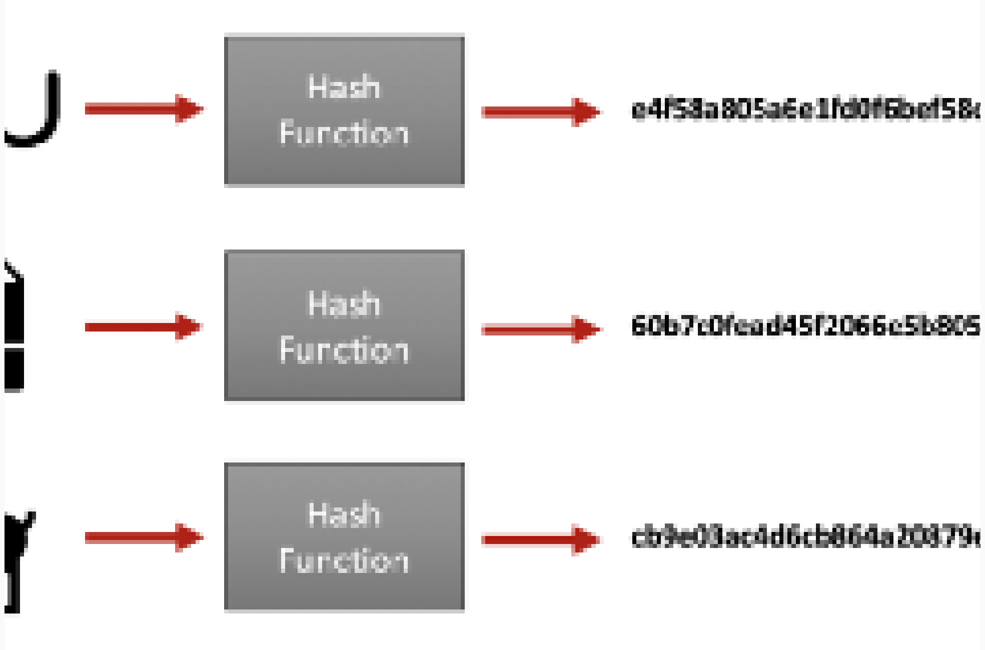
Also tagged Malware Analysis

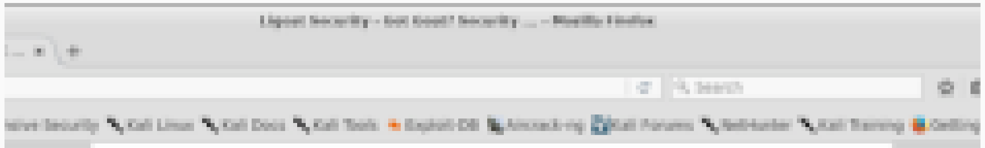
Fifty Shades of Malware Hashing

Thomas Roccia

Sep 29 · 6 min read ★

71





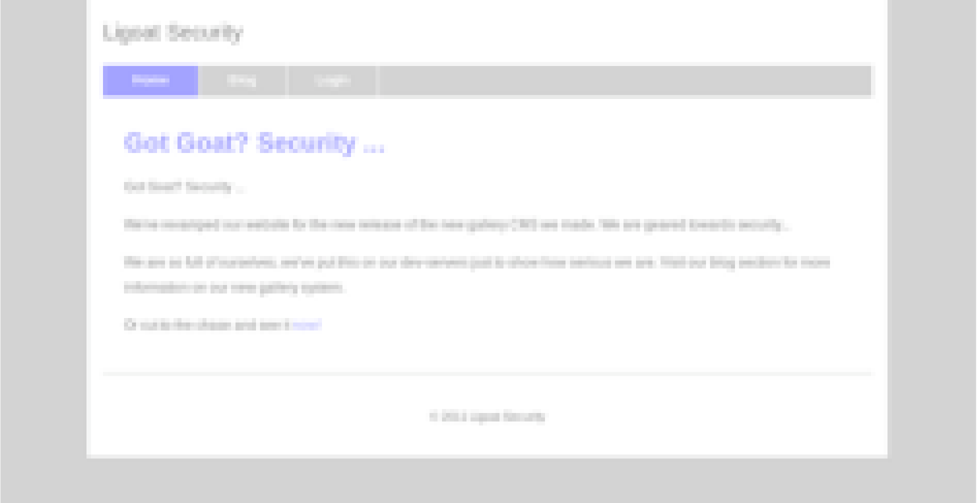
Related reads

VulnHub — Kioptrix: Level 3

Mike Bond

Jun 1, 2018 · 14 min read

270



Ligoat Security

Got Goat? Security ...

Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it here!

© 2011 Ligoat Security