**Universidad Nacional de Costa Rica**

**Escuela de Informática**

**A black and red sign with white text

Description automatically generated**

**Seguridad Informática**

**PenTest**

**PenTest 1: Ataque IP Publica**

**Integrantes:**

**Esteban Chinchilla Brenes, 1-1676-0048**

**Profesor:**

**Henry Guevara Guevara**

**I Ciclo, 2024**

# Herramientas y aspectos del equipo con el cual se realizará las pruebas

Herramientas:

* BurpSuite
* Chrome: Herramientas de desarrollador

Equipo:

* Sistema operativo: Windows 10
* IP publicas usadas durante las pruebas
  + A screenshot of a phone number

    Description automatically generated[05/20/2024: 11:03P.M]
  + []

# Etapa 1 [05/20/2024]

Objetivo: IP 201.195.246.8

Obtener credenciales e información util de los portales que implementa la VM desplegada en la IP proporcionada.

Tras una rápida verificación al código fuente del portal de bienvenida se obtienen las siguientes credenciales y versiones utilizadas por las aplicaciones.

OWASP WebGoat

Version: 5.4+SVN

Language: Java

User Credentials (username/password): guest/guest

User Credentials (username/password): user/user

User Credentials (username/password): basic/basic

Admin Credentials (username/password): webgoat/webgoat

OWASP WebGoat.NET

Version: 2012-07-05

Language: C# ASP.NET

User Credentials (username/password): bob@ateliergraphique.com/123456

OWASP ESAPI Java SwingSet Interactive

Version: 1.0.1+SVN

Language: Java

OWASP Mutillidae II

Version: 2.6.24

Language: PHP

User Credentials (username/password): user/user

Admin Credentials (username/password): admin/admin

OWASP RailsGoat

Version: Git

Language: Ruby on Rails

<b>Admin Credentials (username/password): </b>admin@metacorp.com/admin1234<br />

<b>User Credentials (username/password): </b>jack@metacorp.com/yankeessuck<br />

<b>Link: </b><a href="http://railsgoat.cktricky.com/">home page</a><br />

</div></td>

<td><a href="javascript:animatedcollapse.toggle('owaspbricks')"><img src="images/Knob\_Add.png" width="20px" height="20px" border="0" title="More Info" /></a><a href="owaspbricks">OWASP Bricks</a>

<div id="owaspbricks" style="width: 400px; background: #D2FBFF; display:none">

<b>Version: </b>2.2+SVN<br />

<b>Language: </b>PHP<br />

<b>Link: </b><a href="http://sechow.com/bricks/">home page</a><br />

</div></td>

</tr>

<tr>

<td ><a href="javascript:animatedcollapse.toggle('shepherd')"><img src="images/Knob\_Add.png" width="20px" height="20px" border="0" title="More Info" /></a><a href="shepherd/">OWASP Security Shepherd</a>

<div id="shepherd" style="width: 400px; background: #D2FBFF; display:none">

<b>Version: </b>2.4+Git<br />

<b>Language: </b>Java<br />

<b>Admin Credentials (username/password): </b>admin/password<br />

<b>Link: </b><a href="https://www.owasp.org/index.php/OWASP\_Security\_Shepherd">home page</a><br />

</div></td>

<td ><a href="javascript:animatedcollapse.toggle('ghost')"><img src="images/Knob\_Add.png" width="20px" height="20px" border="0" title="More Info" /></a><a href="ghost">Ghost</a>

<div id="ghost" style="width: 400px; background: #D2FBFF; display:none">

<b>Language: </b>PHP<br />

<b>User Credentials (username/password): </b>test/test<br />

<b>User Credentials (username/password): </b>anonymous/anonymous<br />

<b>Admin Credentials (username/password): </b>admin/admin<br />

<b>Link: </b><a href="http://www.gh0s7.net">home page</a><br />

</div></td>

</tr>

<tr>

<td ><a href="javascript:animatedcollapse.toggle('MCIR')"><img src="images/Knob\_Add.png" width="20px" height="20px" border="0" title="More Info" /></a><a href="MCIR">Magical Code Injection Rainbow</a>

<div id="MCIR" style="width: 400px; background: #D2FBFF; display:none">

<b>Version: </b>2014-08-20+Git<br />

<b>Language: </b>PHP<br />

<b>Link: </b><a href="https://github.com/SpiderLabs/MCIR">home page</a><br />

</div></td>

<td ><a href="javascript:animatedcollapse.toggle('bwapp')"><img src="images/Knob\_Add.png" width="20px" height="20px" border="0" title="More Info" /></a><a href="bWAPP">bWAPP</a>

<div id="bwapp" style="width: 400px; background: #D2FBFF; display:none">

<b>Version: </b>1.9+Git<br />

<b>Language: </b>PHP<br />

<b>User Credentials (username/password): </b>bee/bug<br />

<b>Link: </b><a href="http://www.itsecgames.com/">home page</a><br />

</div></td>

</tr>

<tr>

<td><a href="javascript:animatedcollapse.toggle('dvwa')"><img src="images/Knob\_Add.png" width="20px" height="20px" border="0" title="More Info" /></a><a href="dvwa">Damn Vulnerable Web Application</a>

<div id="dvwa" style="width: 400px; background: #D2FBFF; display:none">

<b>Version: </b>1.8+GIT<br />

<b>Language: </b>PHP<br />

<b>User Credentials (username/password): </b>user/user<br />

<b>Admin Credentials (username/password): </b>admin/admin<br />

<b>Link: </b><a href="http://www.dvwa.co.uk/">home page</a><br />

</div></td>