Difficulty

EASY

Conventions

- requires given Linux commands to be executed with root privileges either directly as a root user or by use of sudo command
- requires given Linux commands to be executed as a regular non-privileged user

Instructions

Accessthe default application for taking screenshots on Gnome.

Get G Suite.

Screenshot
Difficulty
EASY

Conventions
- $ ____ requires given Linux commands to be executed with root privileges either directly as a root user or by use of sudo command
- $ ____ requires given Linux commands to be executed as a regular non-privileged user

Instructions

Screenshot is a default application for taking screenshots on Gnome.

G Suite. Work better together.
Difficulty

EASY

Conventions

- $: requires given Linux commands to be executed with root privileges
- requires Linux commands to be executed as a regular non-

privileged user

Instructions

Screenshot

Screenshot is a default application for taking screenshots on Gnome

Get G Suite. Work better together.
Difficulty

EASY

Conventions

- **#**: requires given Linux commands to be executed with root privileges either directly as a root user or by use of sudo command
- **$**: requires given Linux commands to be executed as a regular non-privileged user

Instructions

Get G Suite. Work better together.

Screenshot

is a default application for taking screenshots on Gnome.
Difficulty
EASY

Conventions
- # requires given Linux commands to be executed with root privileges either directly as a root user or by use of sudo command
- $ requires given Linux commands to be executed as a regular non-privileged user

Instructions

Screenshot

A default application for taking screenshots on Gnome.

G Suite.
Work better together.

LinuxConfig.org website uses cookies to draw up without audience statistics and measurements and offer you services and offers adapted to your interests. By continuing to browse the site without changing your settings you are agreeing to our use of cookies. For more information visit https://linuxconfig.org/privacy | Accept
Vulnerability: SQL Injection

User ID:

ID: or 1=1
First name: admin
Surname: admin

ID: or 1=1
First name: Gordon
Surname: Brown

ID: or 1=1
First name: Hack
Surname: Me

ID: or 1=1
First name: Pablo
Surname: Picasso

ID: or 1=1
First name: Bob
Vulnerability: SQL Injection

User ID: [Submit]

- ID: ' or 1=1
  First name: admin
  Surname: admin

- ID: ' or 1=1
  First name: Gordon
  Surname: Brown

- ID: ' or 1=1
  First name: Hack
  Surname: Me

- ID: ' or 1=1
  First name: Pablo
  Surname: Picasso

- ID: ' or 1=1
  First name: Bob

SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
Vulnerability: SQL Injection

User ID: [Submit]

ID: 1 or 1=1
First name: admin
Surname: admin

ID: 1 or 1=1
First name: Gordon
Surname: Brown

ID: 1 or 1=1
First name: Hack
Surname: Me

ID: 1 or 1=1
First name: Pablo
Surname: Picasso

ID: 1 or 1=1
First name: Bob
Vulnerability: SQL Injection

User ID: [Input Field]

- ID: ' or 1=1
  - First name: admin
  - Surname: admin

- ID: ' or 1=1
  - First name: Gordon
  - Surname: Brown

- ID: ' or 1=1
  - First name: Jack
  - Surname: Mac

- ID: ' or 1=1
  - First name: Pablo
  - Surname: Picasso

- ID: ' or 1=1
  - First name: Bob
Vulnerability: SQL Injection

User ID: 
Submit

ID: or 3+1
First name: admin
Surname: admin

ID: or 3+4
First name: Gordon
Surname: Brown

ID: or 3+3
First name: Hack
Surname: Me

ID: or 3+2
First name: Pablo
Surname: Picasso

ID: or 3+1
First name: Bob
Vulnerability: SQL Injection

User ID: [Submit]

<table>
<thead>
<tr>
<th>ID</th>
<th>First name</th>
<th>Surname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>2</td>
<td>Gordon</td>
<td>Brown</td>
</tr>
<tr>
<td>3</td>
<td>Mark</td>
<td>Me</td>
</tr>
<tr>
<td>3</td>
<td>Pablo</td>
<td>Picasso</td>
</tr>
<tr>
<td>3</td>
<td>Bob</td>
<td></td>
</tr>
</tbody>
</table>