

نمایش اطلاعات سیستم عامل هدف

- 〈1〉 - نمایش نام نسخه سیستم عامل
- 〈2〉 - نمایش اطلاعات مدل پردازنده
- 〈3〉 - نمایش نام کامپیوتر ↔ Hostname
- 〈4〉 - نمایش نام کاربری که وارد سیستم شده است

اجرای دستورات روی سیستم عامل هدف

- 〈5〉 - دکمه خاموش شدن ↔ poweroff
- 〈6〉 - دکمه شروع مجدد ↔ restart
- 〈7〉 - دکمه قفل کردن ↔ Lock
- 〈8〉 - دکمه بستن صدا ↔ Mute
- 〈9〉 - دکمه باز کردن صدا ↔ Unmute
- 〈10〉 - دکمه خالی کردن سطل زباله ↔ emptybin
- 〈11〉 - دکمه روشن کردن صفحه نمایش ↔ Monitor On
- 〈12〉 - دکمه خاموش کردن صفحه نمایش ↔ Monitor Off

اجرای دستورات دلخواه با فرم nircmd.dll

مانند این چند دستور :

- beep 500 1000 تولید صدایی با فرکانس 500 و به مدت 1 ثانیه در سیستم هدف ➔
- setsysvolume 65535 تنظیم صدای سیستم هدف به عدد 65535 یعنی 100% صدا ➔
- cdrom open/close باز کردن و بستن درایو نوری سیستم هدف ➔

پخش تلفظ متن نوشته شده در سیستم هدف

هر چیزی که در این کادر نوشته شود بالافصله در سیستم هدف به صورت صوت پخش میشود

The screenshot shows a web browser window with the URL `127.0.0.1:5000/profile`. The page has a dark theme with a light blue header bar. At the top center is a circular profile icon with a person icon inside. Below it, the word "Profile" is written. On the left side, there is a large circular placeholder for a user's profile picture, with a small "+" icon at the bottom right of the circle. To the right of the placeholder, the text "Welcom My Friend" is displayed in a bold, blue font. Below this, there are several input fields and labels:

- Fullscreen icon
- Home icon
- Back icon
- Forward icon
- Search icon
- Refresh icon
- Stop icon
- Help icon
- More icons

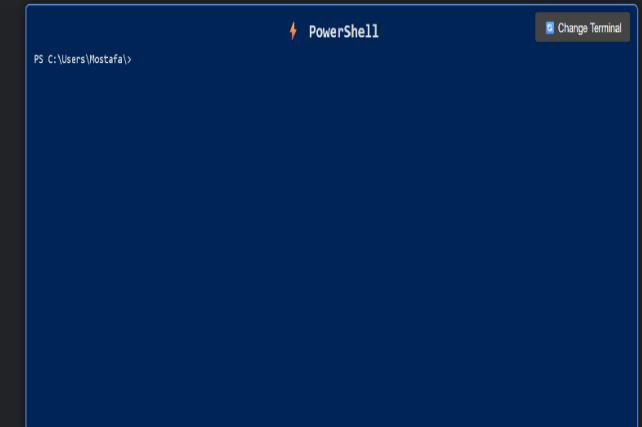
Fullscreen	Home	Back	Forward	Search	Refresh	Stop	Help	More
------------	------	------	---------	--------	---------	------	------	------

Fullname:	
Username:	guest
Password:	*****
Email:	example@gmail.com
Token:	d605be870ae9e0ce35187baafc39ed78
IP_Port:	http://127.0.0.1:5000

Edit

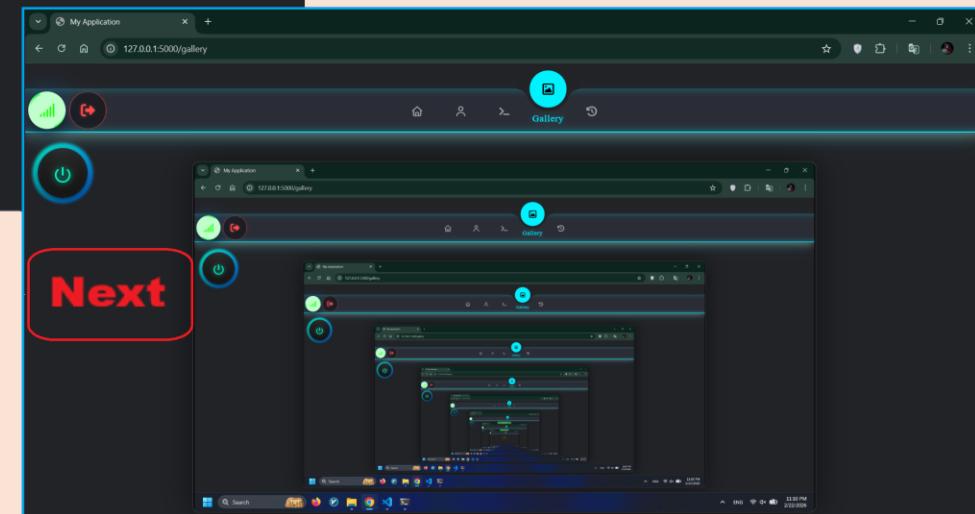
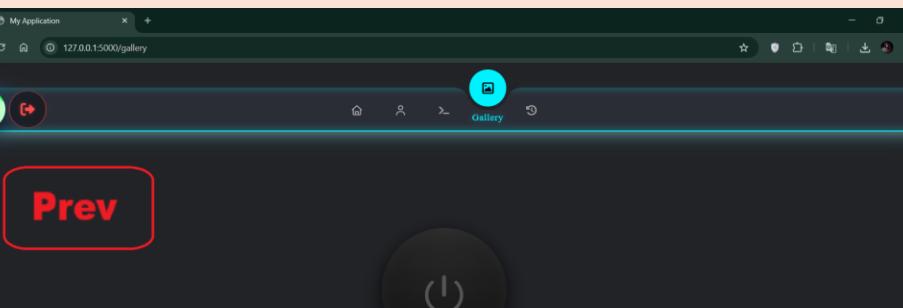
بخش پروفایل

+ ← دکمه برای تغییر آواتار پیشفرض
← نام کامل کاربر ← Fullname
← نام کاربری که یکتا است ← Username
← رمز عبور ← Password
← ایمیل کاربر ← Email
← کد یکتایی که در بد افزار باید استفاده شود تا ارتباط با سرور برقرار شود ← Token
← آی پی یا نام دامنه ← IP_Port
← دکمه ای برای ویرایش اطلاعات پروفایل ← Edit



بخش ترمینال

با کلیک روی دکمه Change Terminal نوع ترمینال عوض میشود
با زدن دستور cd در هر دو ترمینال آدرس مسیر فعلی در سیستم هدف ذخیره میشود و جایگزین مسیر پیشفرض میشود



بخش نمایش

اسکرین شات های گرفته شده از سیستم هدف تقریباً به فاصله 1 ثانیه فرستاده میشوند
با کلیک روی دکمه PowerShell فرایند گرفتن عکس از صفحه کاربر شروع میشود و با کلیک دوباره روی همان دکمه فرایند متوقف میشوند

The screenshot shows a web application interface with a dark theme. At the top, there's a header bar with icons for refresh, search, and other browser functions. Below the header, a navigation bar includes a home icon, a circular 'History' button with a refresh symbol, and a magnifying glass icon for search.

The main content area is titled '**>_ Command History**'. It displays four separate command history entries:

- DLL**:
command: `mutesysvolume 1`
result: Command executed successfully
- SAY**:
command: `welcom to my site`
result: I said to them: welcom to my site
- PS**:
command: `cd`
result: C:\Users\Mostafa\
- CMD**:
command: `where gcc`
result: C:\msys64\ucrt64\bin\gcc.exe

Each entry includes a timestamp at the top right: ۱۴۰۴/۱۲/۰۷، ۲۱:۰۳:۰۵ for DLL, SAY, and PS; and ۱۴۰۴/۱۲/۰۷، ۲۱:۰۴:۴۰ for CMD.

بخش تاریخچه

در این بخش تمام دستورات ارسال شده به بدافزار به همراه جزئیات کامل نمایش داده می‌شوند. همچنین در این بخش امکان جستجوی دستورات فراهم است که میتواند در پیدا کردن دستور شما کمک کننده باشد.