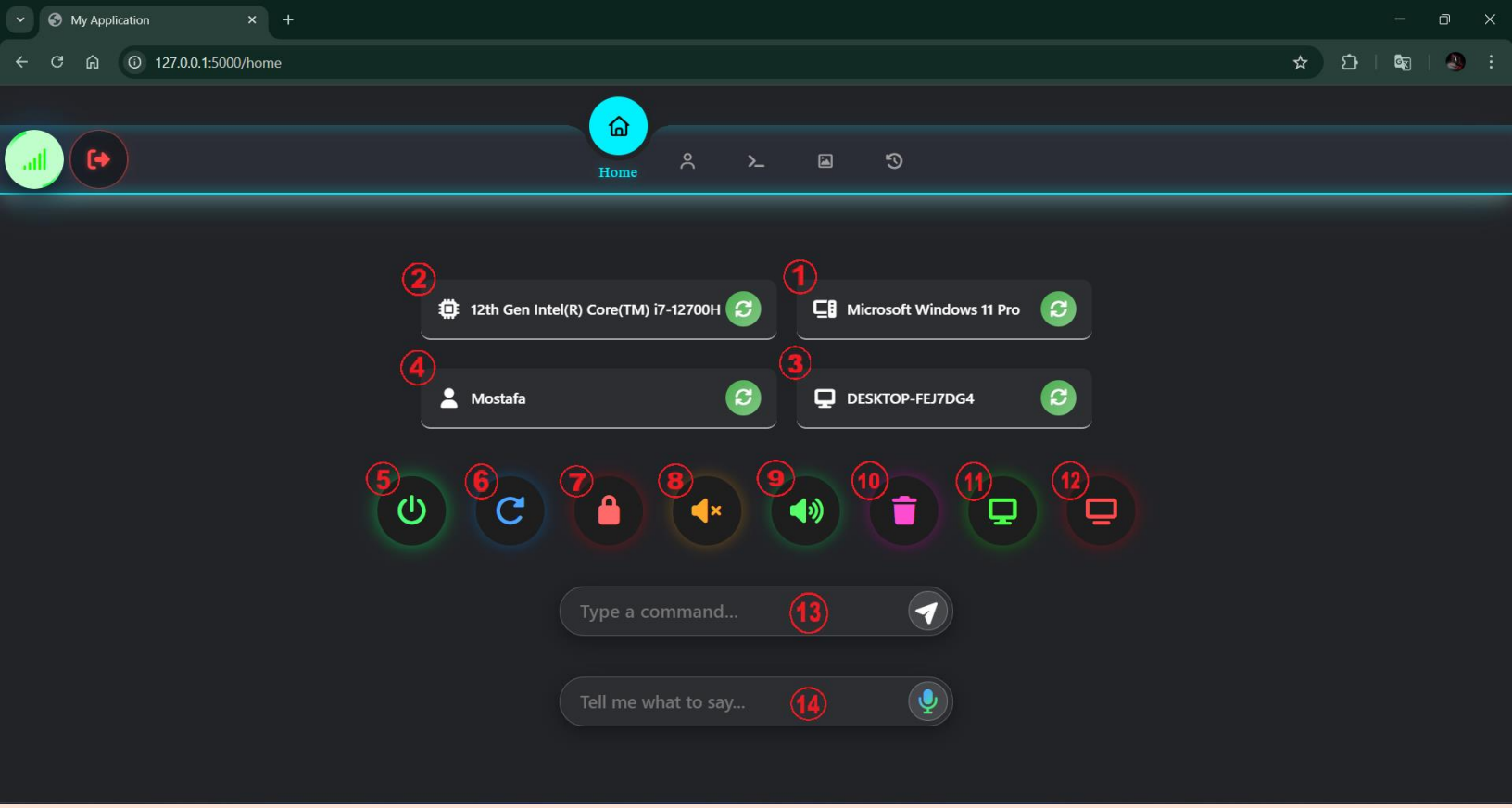


نمایش اطلاعات سیستم عامل هدف

⟨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

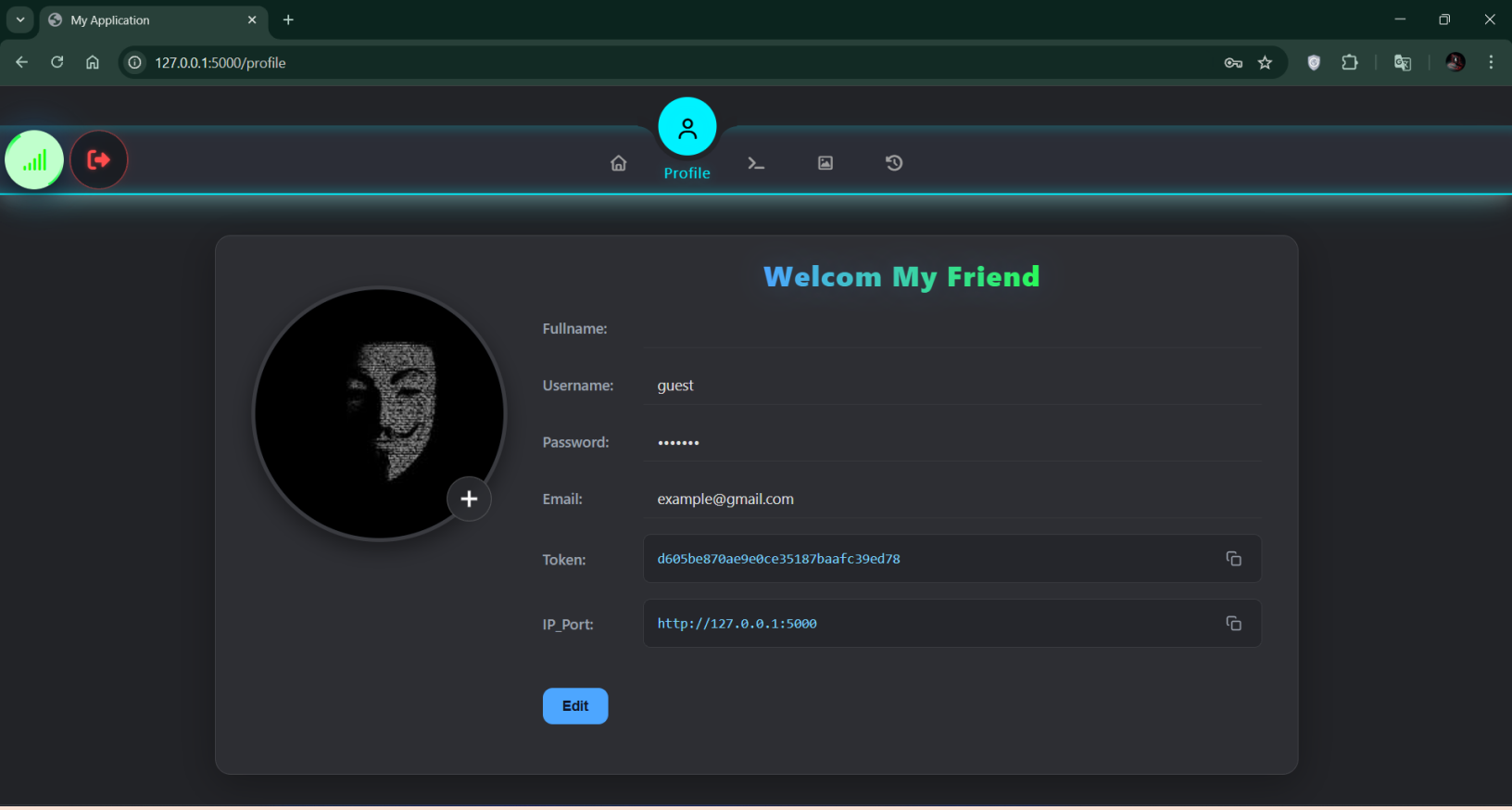
اجرای دستورات دلخواه با فرم nircmd.dll

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 بالافاصله در سیستم هدف به صورت صوت پخش میشود



بخش پروفایل

\+ ⇐ دکمه برای تغییر آواتار پیشفرض

Fullname ⇐ نام کامل کاربر

Username ⇐ نام کاربری که یکتا است

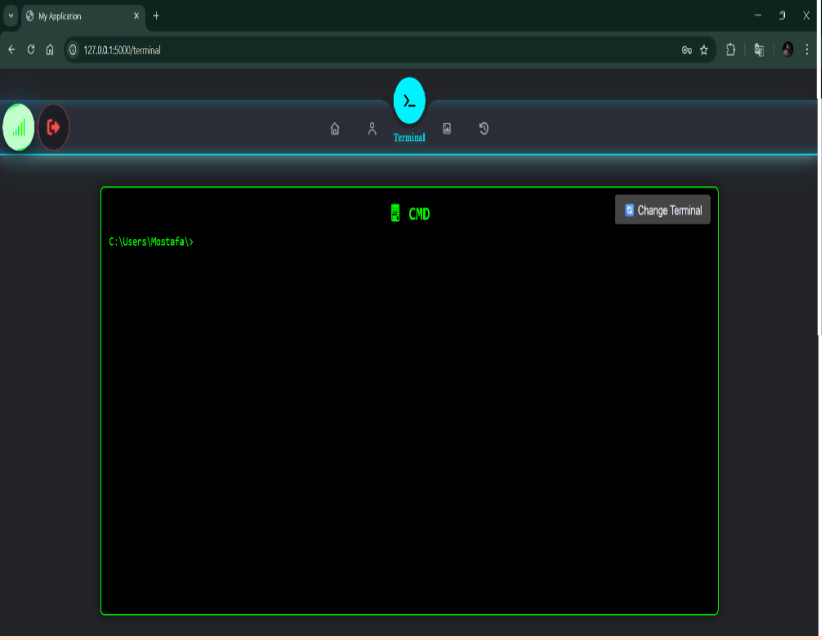
Password ⇐ رمز عبور

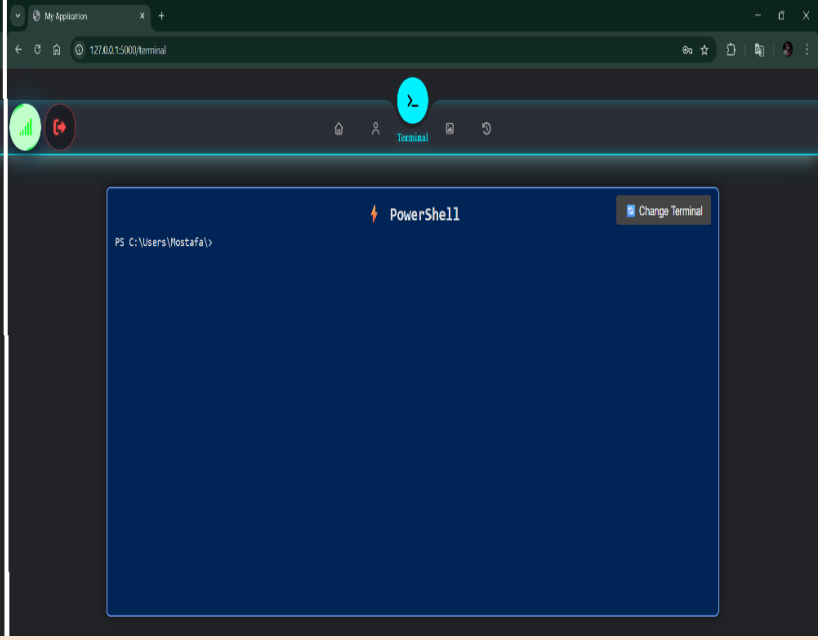
Email ⇐ ایمیل کاربر

Token ⇐ کد یکتایی که در بد افزار باید استفاده شود تا ارتباط با سرور برقرار شود

IP_Port ⇐ آی پی یا نام دامنه

Edit ⇐ دکمه ای برای ویرایش اطلاعات پروفایل

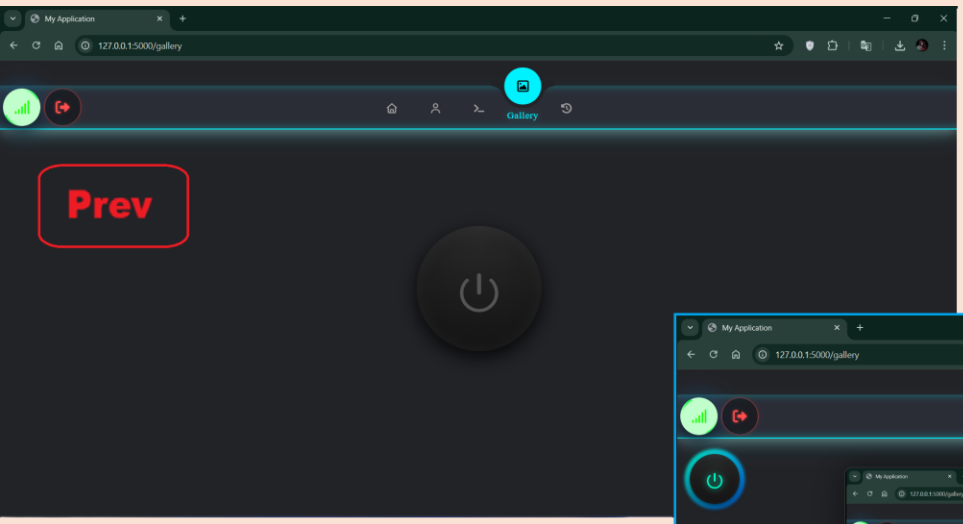


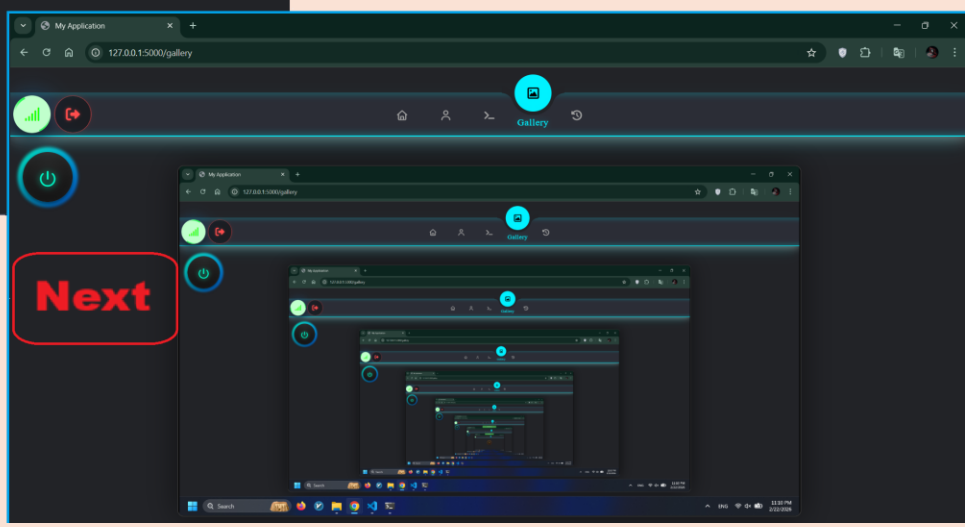


بخش ترمینال

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

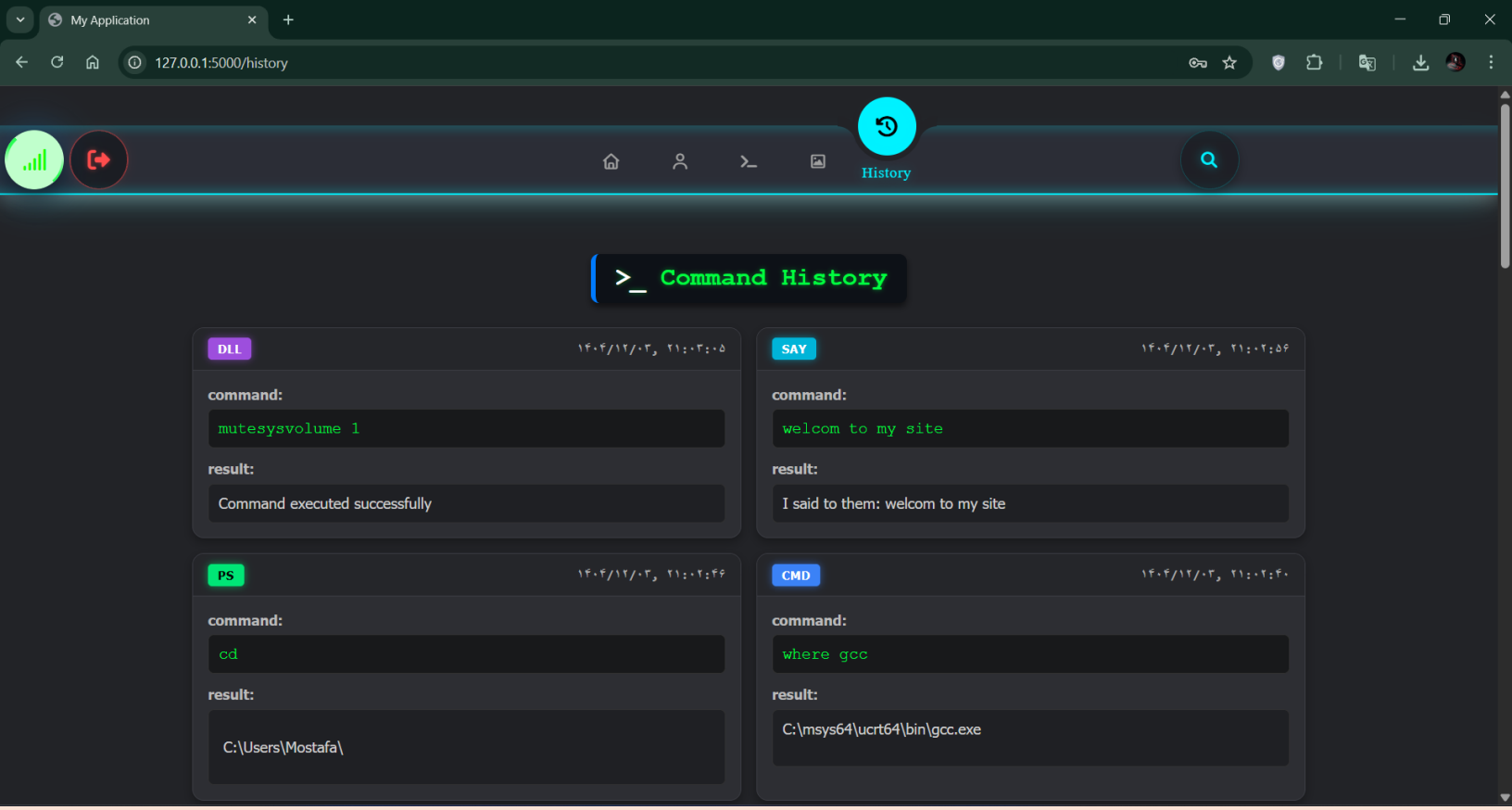




بخش نمایش

اسکرین شات های گرفته شده از سیستم هدف تقریبا به فاصله 1 ثانیه فرستاده میشوند

با کلیک روی دکمه Power فرایند گرفتن عکس از صفحه کاربر شروع میشود و با کلیک دوباره روی همان دکمه فرایند متوقف میشوند



بخش تاریخچه

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