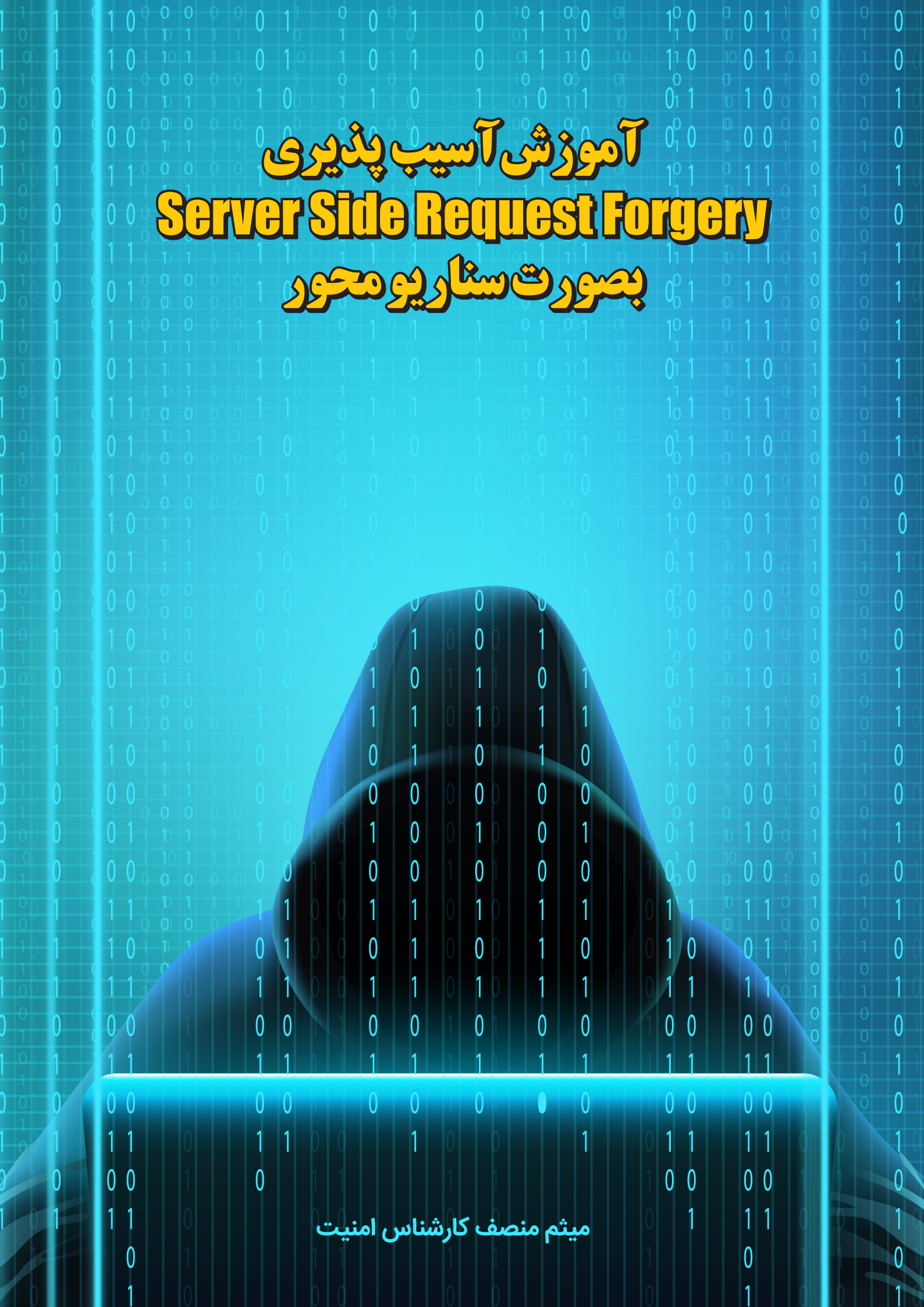
آموزش آسیب پذیری
Server Side Request Forgery
بصورت سناریو محور



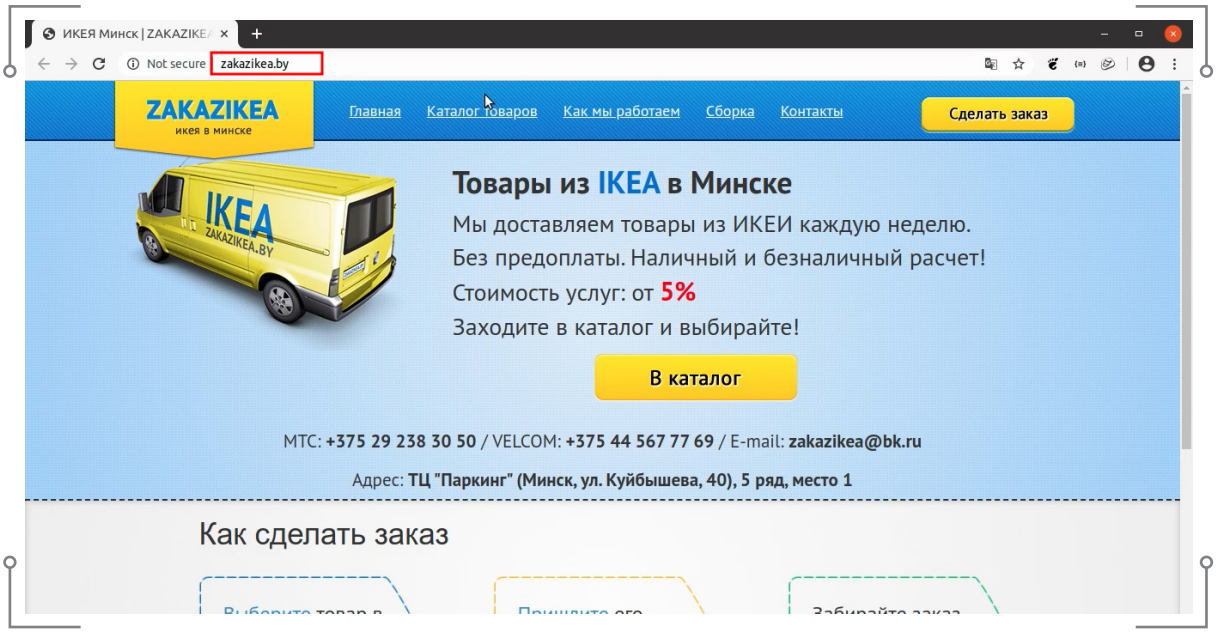
میثم منصف کارشناس امنیت

SSRF چیست ؟

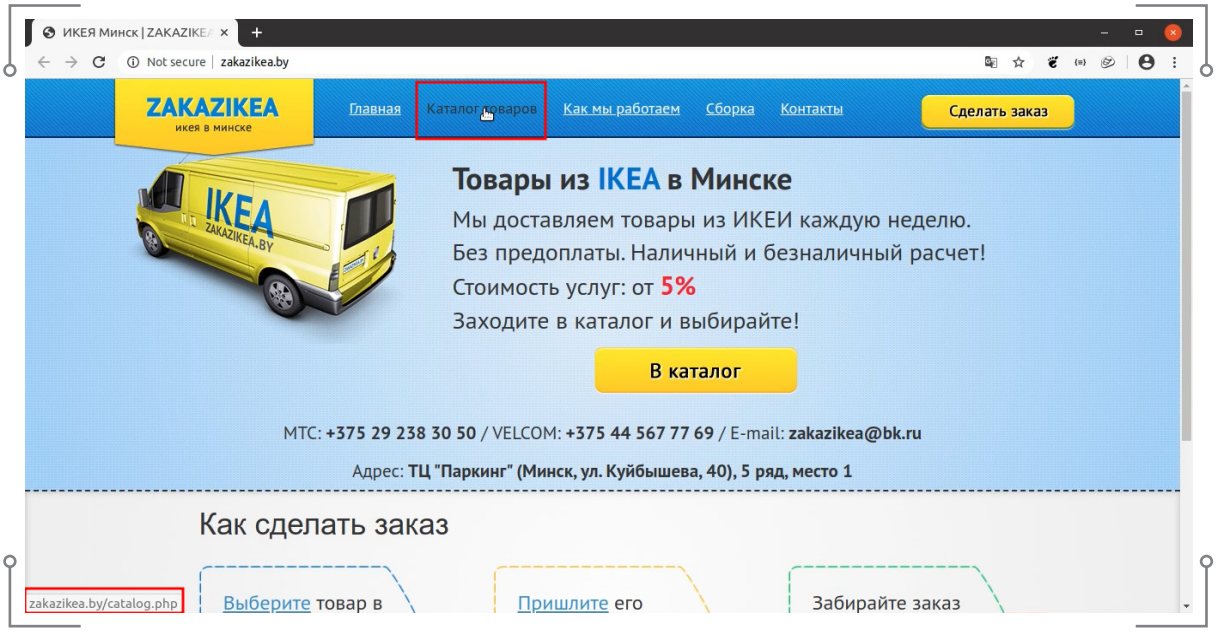
این نوع حمله باعث می‌شود که هکر بتواند درخواست های جعلی از سمت سرور ارسال کند که کاربرد های زیادی که به تشریح آن میپردازیم .

تشخیص آسیب پذیری :

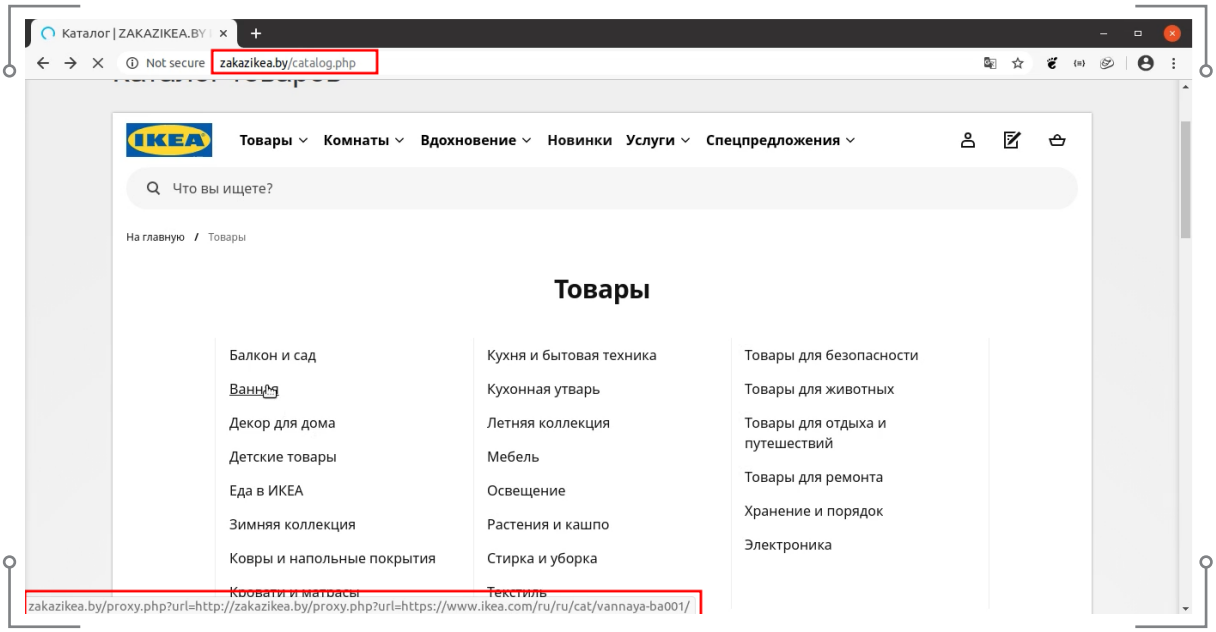
تشخیص این نوع آسیب پذیری نیاز به کسب تجربه دارد و ممکن است در هر قسمتی از سایت رخ بدهد برای اینکه شما این آسیب پذیری را خوب درک کنید من یه تارگت آنلاینی را پیدا کردم که با هم روش کار میکنیم .



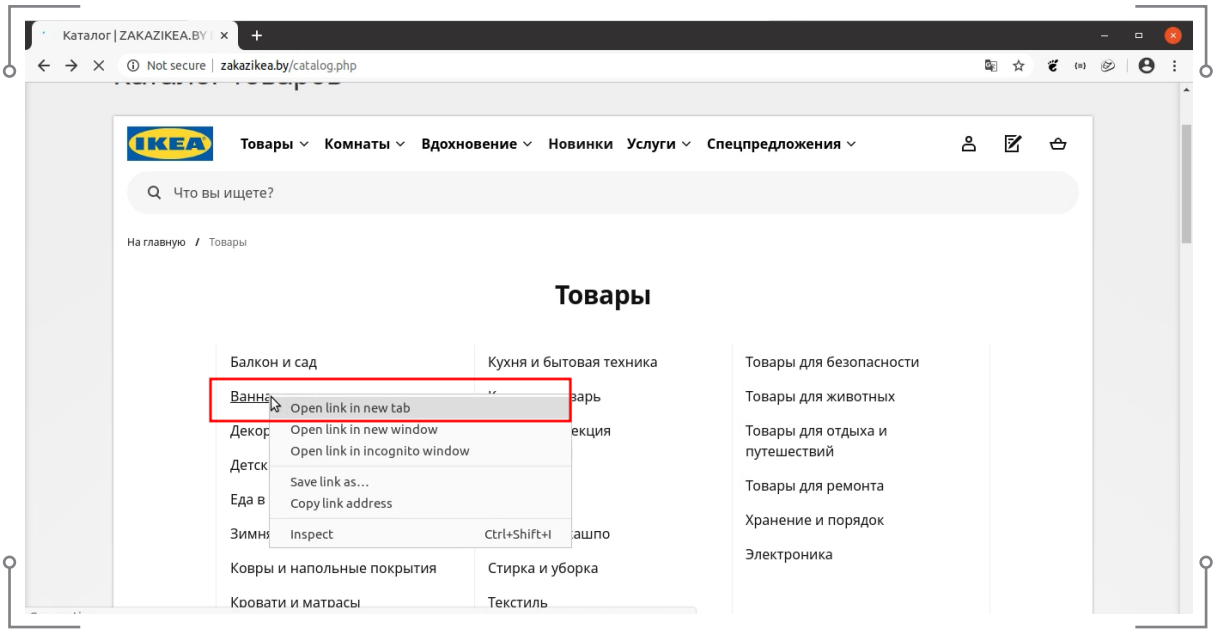
خوب طبق معمول شروع میکنیم به پیدا کردن صفحاتی که بهش بتوانیم مقدار تزریق کنیم من روی این منو کلیک میکنم (زبان روسی بلد نیستم)



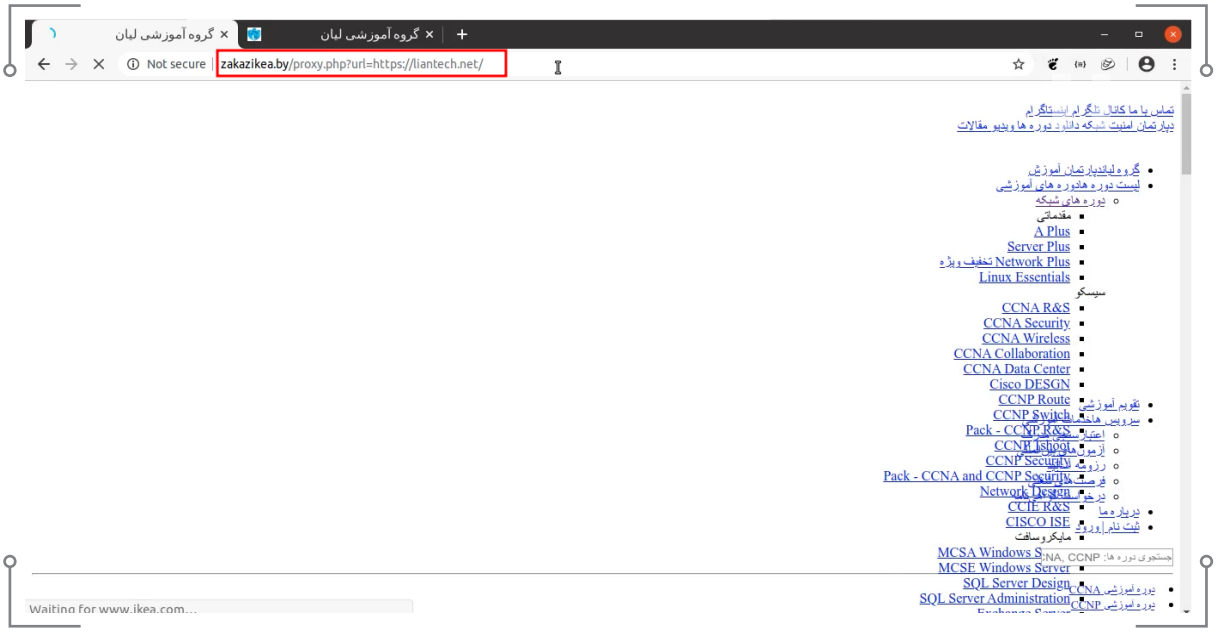
در صفحه‌ای که باز می‌شود روی لینک ها موس را قرار میدم و به قسمت پایین صفحه مرورگر خودم نگاه میکنم .



همانطور که می‌بینید یه صفحه با ورودی پیدا کردم آن را در tab جدید باز میکنم .



در صفحه‌ای باز شده پارمتر url را به آدرس https://liantech.net تغییر میدم .



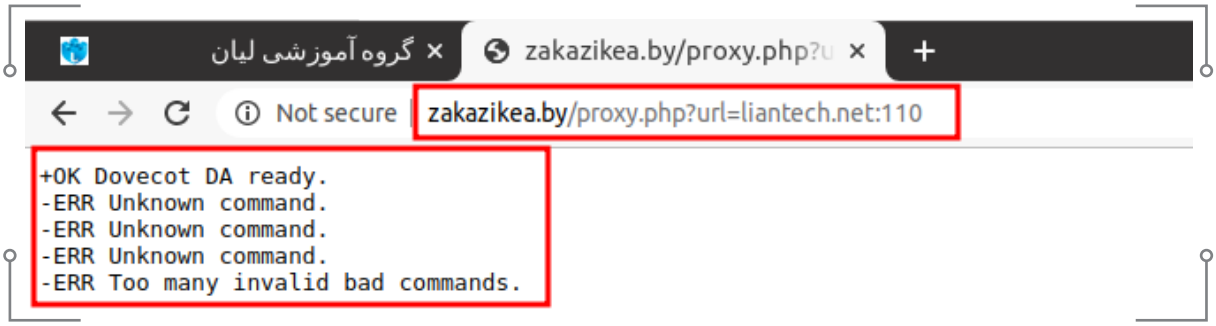
همانطور که در تصویر بالا می‌بینید سایت مورد نظر باز شد.
جالب شد نه الان من از سرور این سایت http://zakazikea.by توانستم سایت ten.hcetnail//:sptth را باز کنم این یعنی که ممکن است سایت مورد نظر آسیب پذیری SSRF را داشته باشد .
خوب حالا بریم ببینیم با این آسیب پذیری چه کارهای را میتوانیم انجام بدیم .

کاربرد اول : استفاده به عنوان Port Scanner

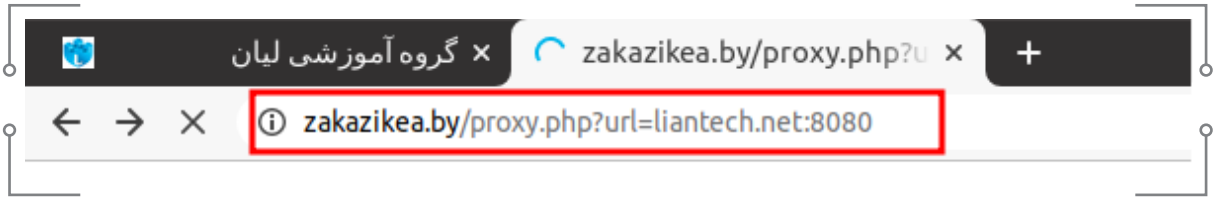
در این حالت هکر میتواند عملیات اسکن کردن پورت ها را از سرور آسیب پذیر انجام دهد و بدون اینکه ردپایی از خود به جا بذارد یا از منابع سیستمی خود استفاده کند.

من الان میخوام ببنیم که آیا پورت ۲۱ در سرور liantech.net باز هست یا خیر ؟

ببینیم پورت ۱۱۰ چطور ؟



خوب ببنیم پورت ۸۰۸۰ باز هست یا خیر ؟



همانطور که در تصویر بالا می‌بینید پورت ۸۰۸۰ باز نیست
خوب خیلی راحت هکر یه ابزار با پایتون می‌نویسد تک تک پورت بررسی میکند .
جالب است بدانید با این حالت میتوان شبکه‌های خصوصی درون شبکه ای را هم اسکن کرد .

کاربرد دوم : دور زدن محدویت های IP

من یادم هست در یک تارگت وقتی میخواستم پنل ادمین را باز کنم به من اجازه دسترسی نمیداد و می‌گفت که IP شما مجاز نمیباشد و چون آسیب پذیر SSRF از تارگت پیدا کرده بودم خیلی راحت به شکل زیر تو پنل مدیریت لاگین کردم . (البته تو این تارگت این امکان نبود)

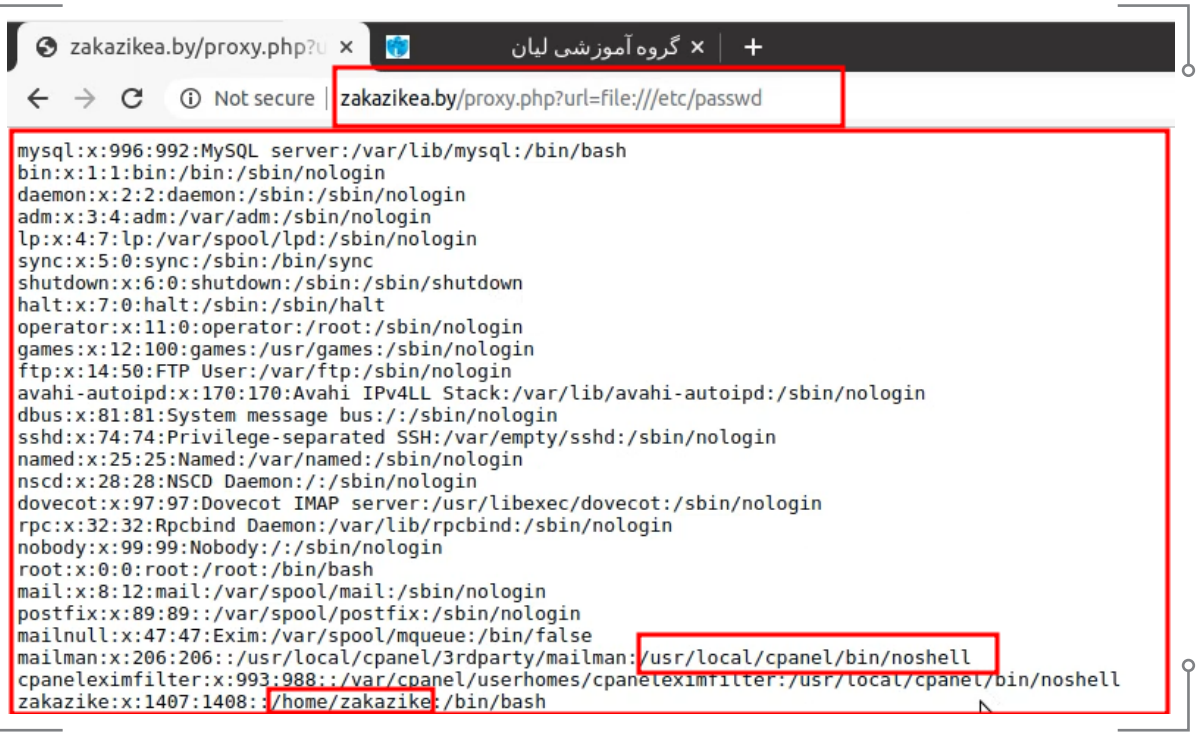
من درخواست به این آدرس http://target.com/admin را دادم و به من پیام شما با این IP امکان دسترسی به این قسمت را ندارید را به من داد . اما با آدرس صفحه آسیب پذیرکه درخواست دادم به شکل زیر پنل مدیریت باز شد .

http://target.com/proxy.php?url=http://localhost/admin

کاربرد سوم : خواندن فایل‌های سرور

شاید قشنگ‌ترین نوع دسترسی از این آسیب پذیری خواندن فایل‌های روی سایت و سرو می باشد که میتوانیم با wrapper file این کار را انجام بدیم .

بریم ببینیم میتوانیم فایل passwd را از سرور بخوانیم ؟

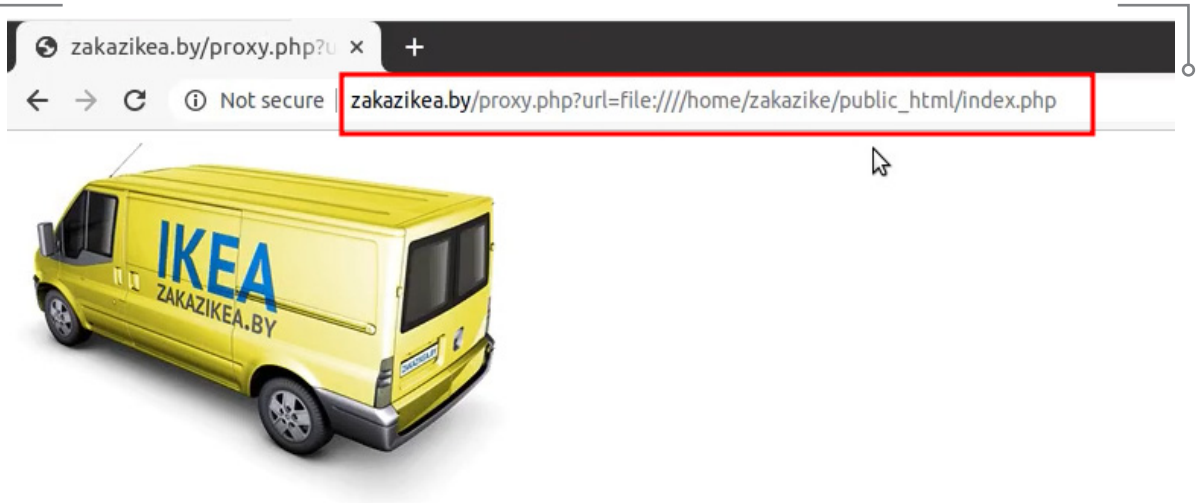


بله جواب داد بسیار هم عالی خوب در ادامه بریم سورس های php سایت را بخوانیم برای این کار شما باید بتوانید مسیر فایل‌ها را تشخیص بدید.

خوب همانطور که در تصویر بالا می‌بینید مسیر cpanel وجود دارد بطور کامل میتونم بگم هاست با cpanel مدیریت می‌شود خوب پایین‌تر هم مسیر خانه این یوز را نمایش میدهد (البته این احتمالاً یک vps شخصی می باشد و یک هاست و دامنه بیشتر ندارد در بعضی از مواقع بخاطر permission ضعیف در سرور میتوان فایل‌های هاست های دیگر داخل سرور را هم خواند) من فکر کنم آدرس فایل index.php باید به شکل زیر باشد :

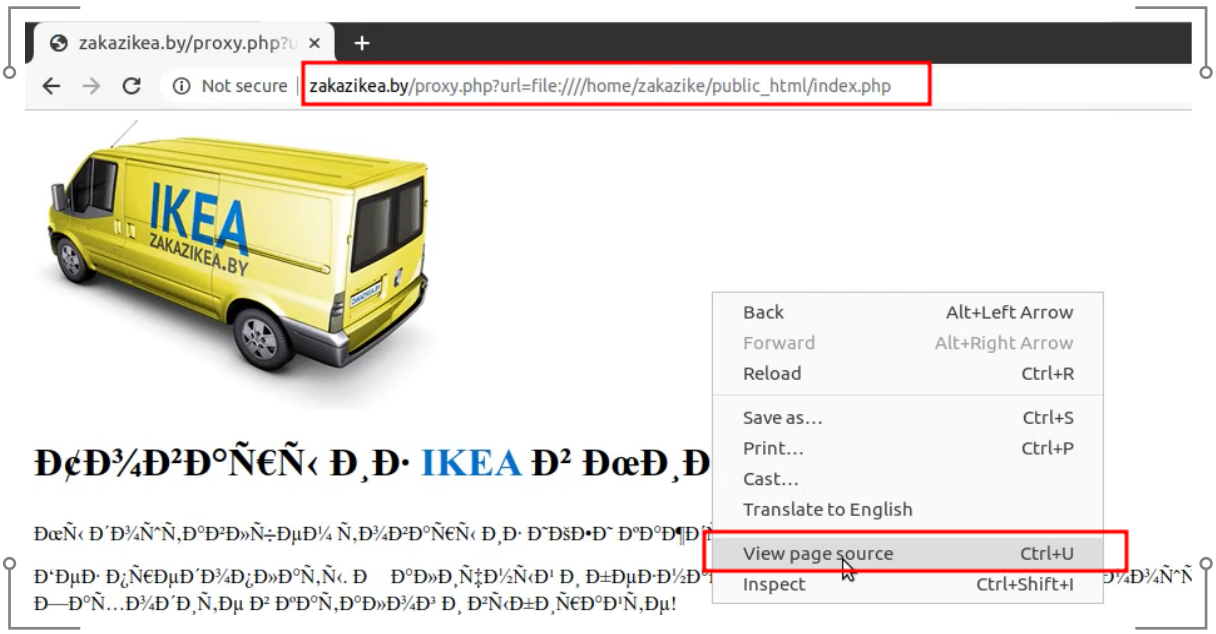
```
/home/zakazike/public_html/index.php
```

خوب با هم تست کنیم ببینیم میتوانیم بخونیم این فایل را ؟

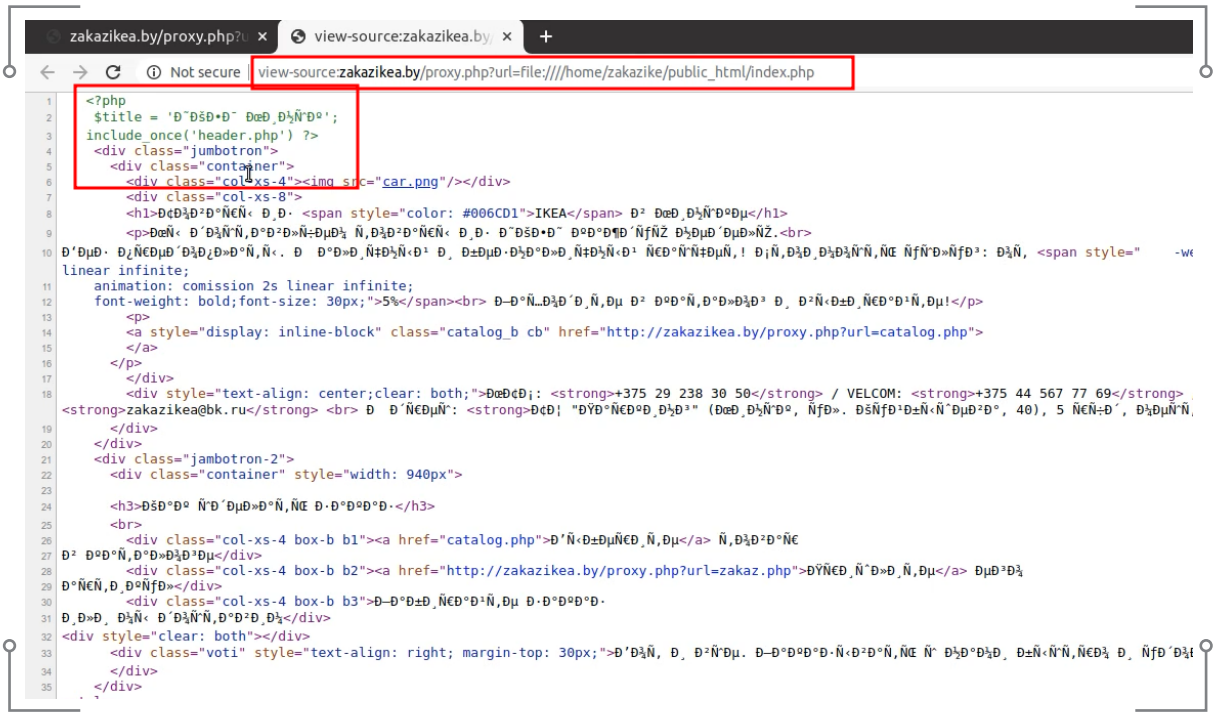


Ð¿Ð¾Ð²Ð°Ñ€Ñ‹ Ð¸Ð· IKEA Ð² ÐœÐ¸Ð½ÑˆÐ°Ðµ

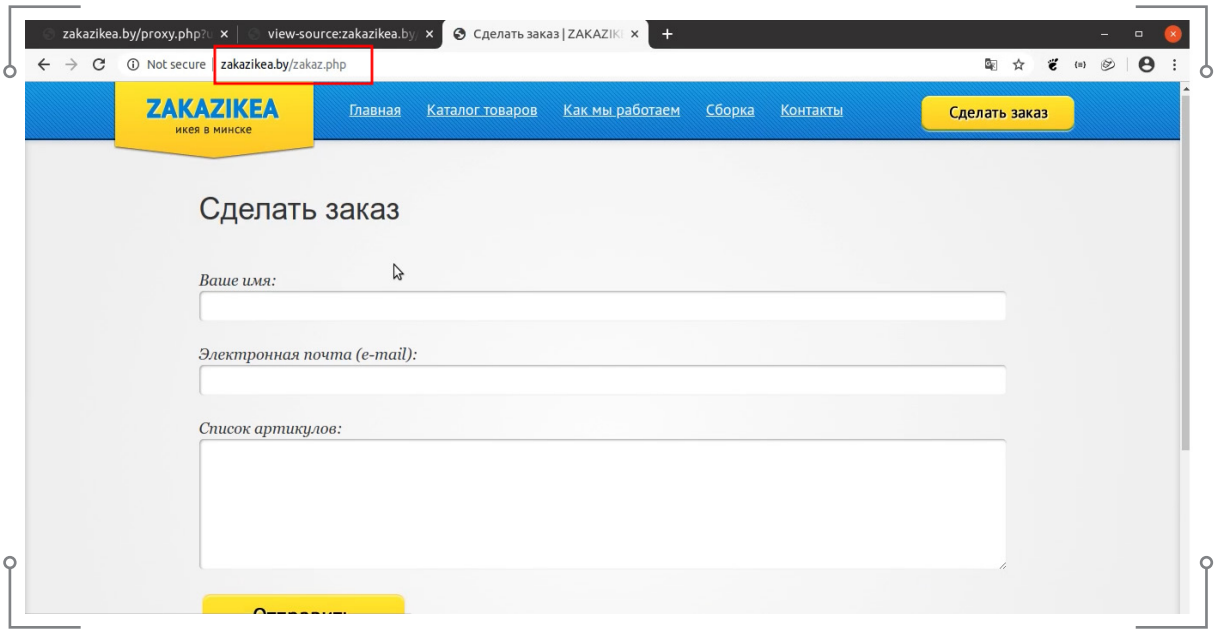
بله جواب داد برای بهتر دیدن خروجی من view page source میگیرم .



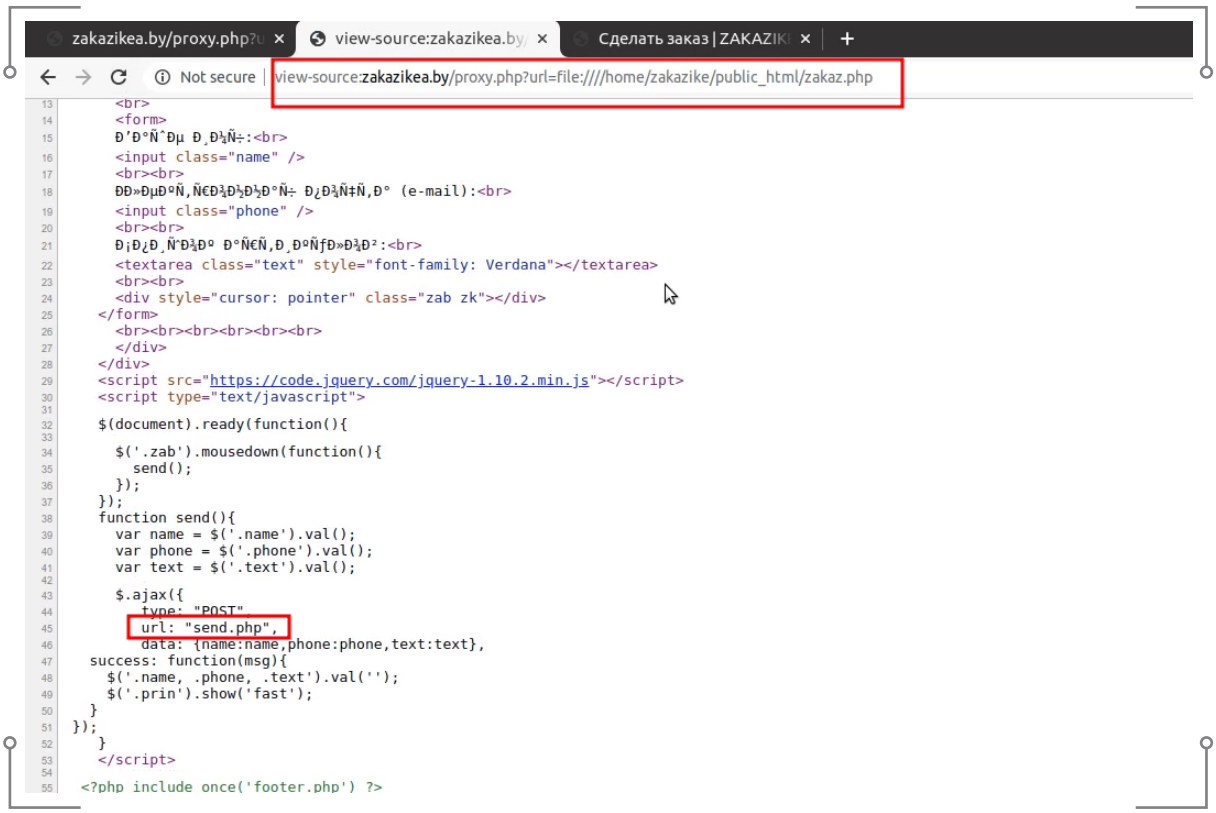
در تصویر پایین همانطور که می‌بینید کدهای php راحت قابل خواندن می باشد.



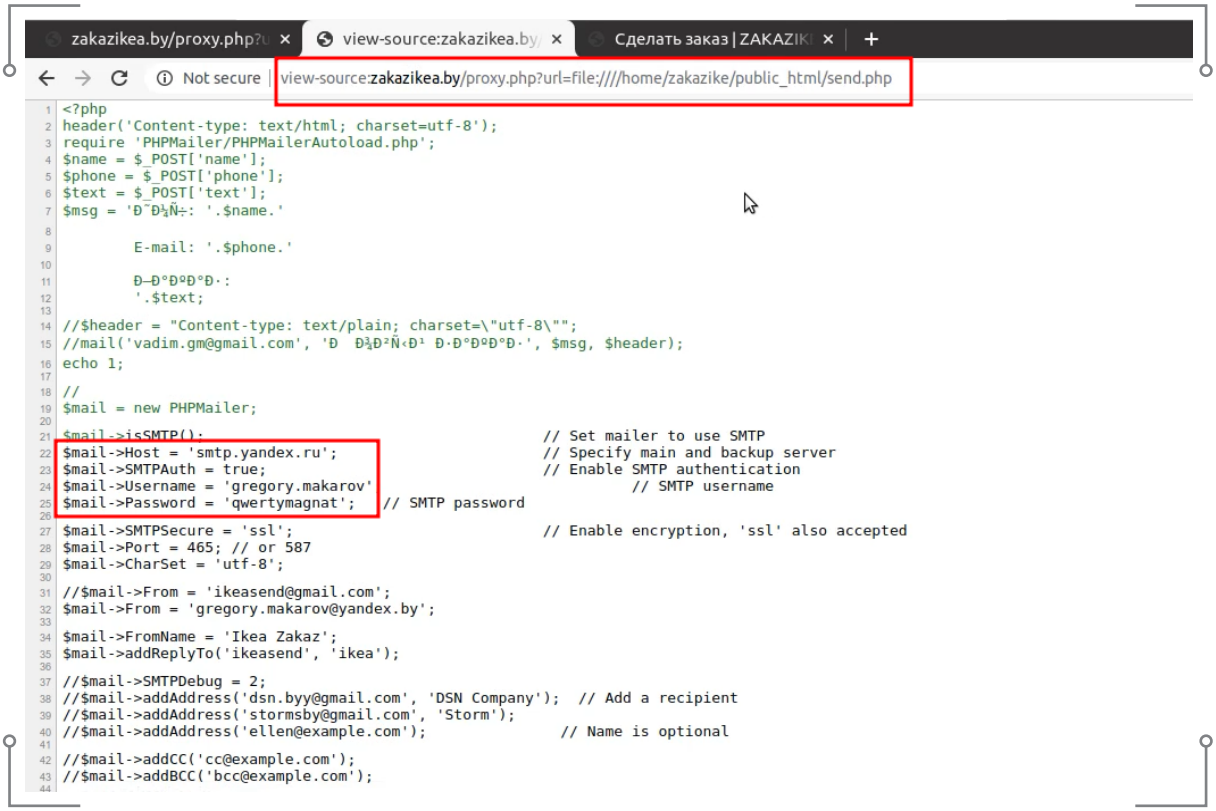
متأسفانه این سایت پنل مدیریت یا چیز های مهمی نداشت اما من با جستجو در صفحات مختلف این سایت توانستم ایمیل سایت را هک کنم با هم این سناریو را دنبال کنیم .
این صفحه تماس با ما هست .



میرم سورس صفحه را میخوانم

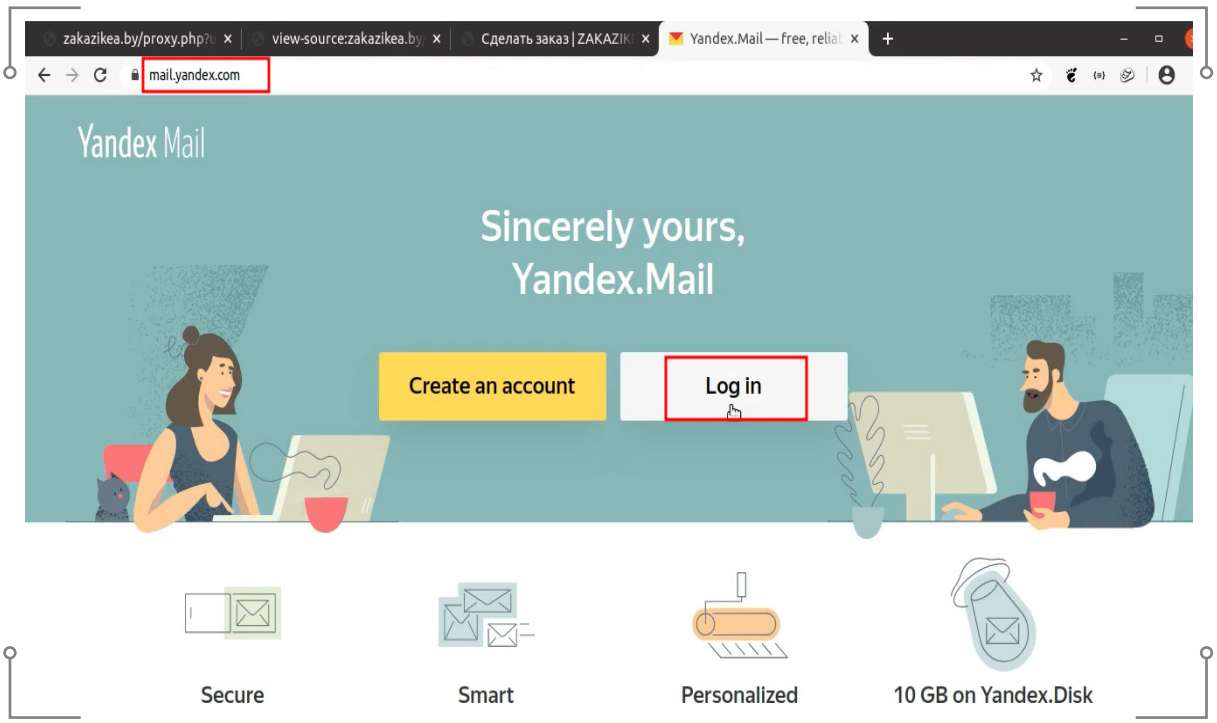


خوب اینجا یه صفحه‌ای دیگه هست این فایل را هم میخوانم (send.php)

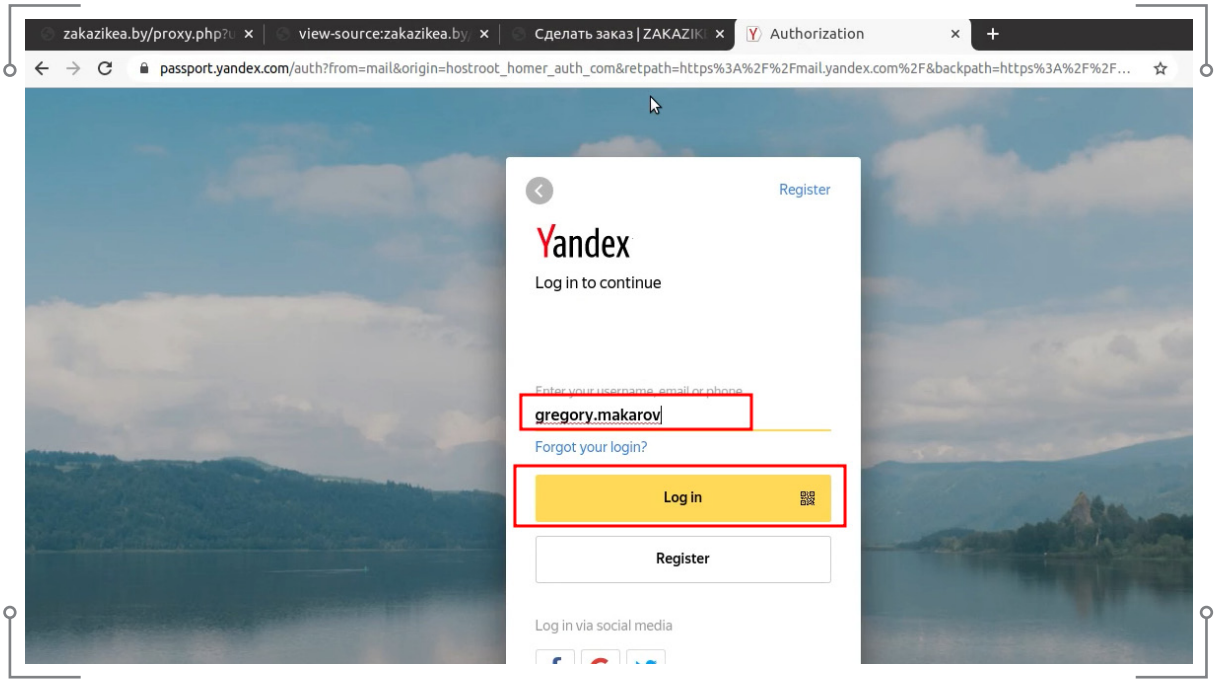


همان‌طور که می‌بینید آدرس سرور ایمیل و یوزر و پسورد را پیدا کردیم بریم ببینیم میتوانیم لاگین کنیم یا خیر ؟

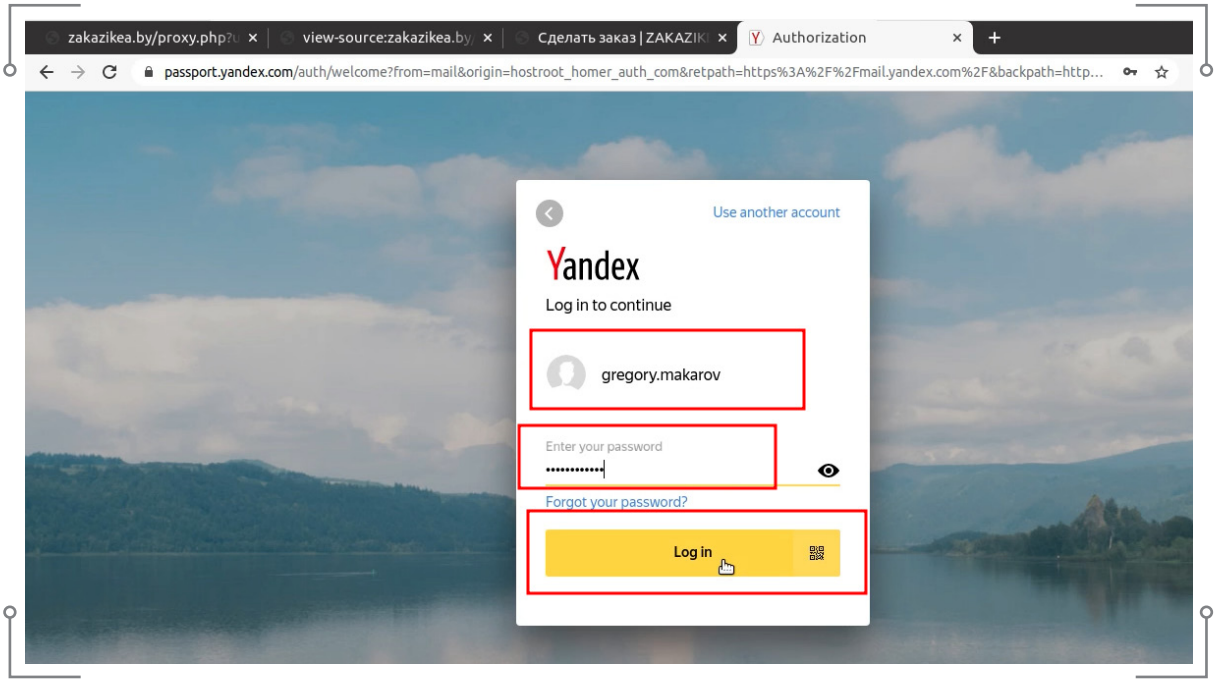
این آدرس ورود به پنل ایمیل است و روی دکمه log in کلیک میکنم



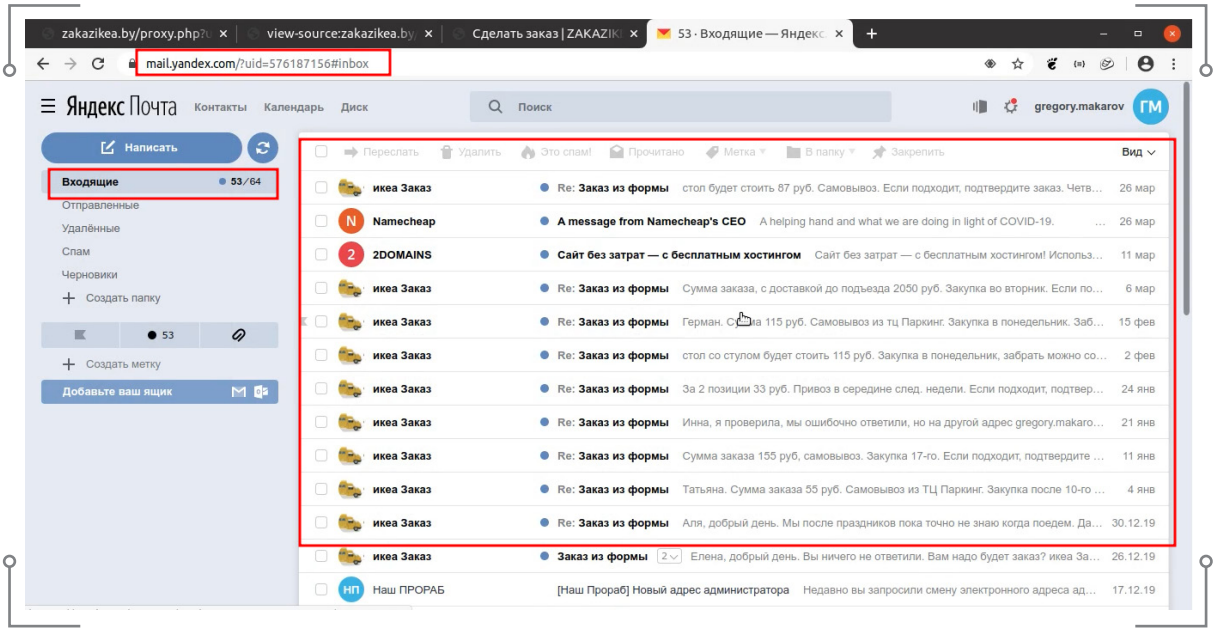
username را وارد میکنم



حالا password را وارد میکنم



و تمام به پنل ایمیل خوش آمدید !



موفق و سربلند باشید

LIANGROUP

Mehrna Rayaneh Lian

تهران، خیابان هویزه، پلاک ۱۲۱، واحد ۲

www.liangroup.net

۰۲۱ ۹۱۰۰۴۱۵۱