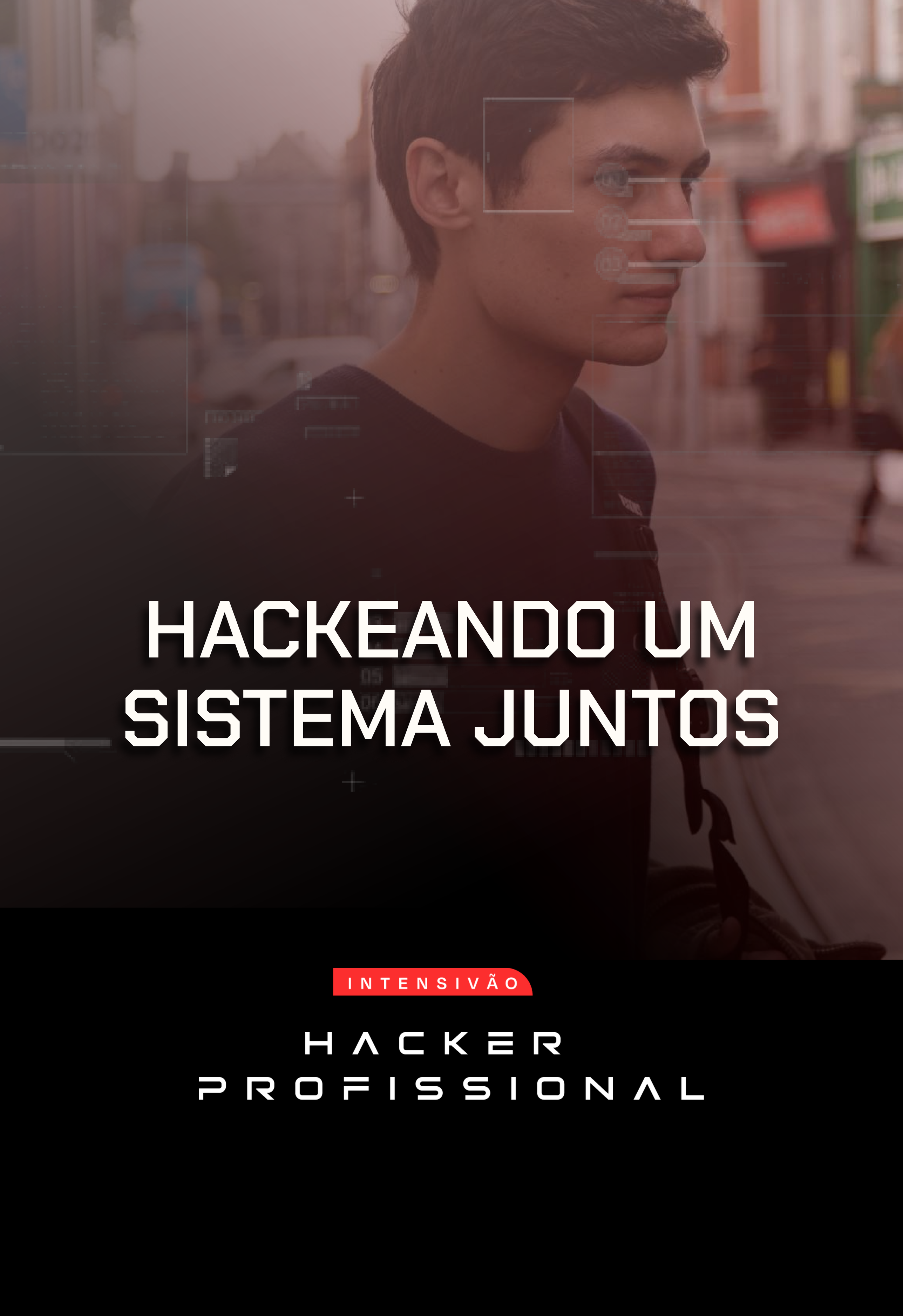


INTENSIVÃO

HACKER PROFISSIONAL

@brunofraga.me

CAT HOJE.TXT

Diante de um problema eu identifiquei uma cortina de fumaça...

Os profissionais estão dificultando o processo de entrada e aprendizado para iniciantes.

Ninguém te fala o caminho do hacking e eu estou disposto a te mostrar esse caminho.

CONHECIMENTO OCULTO

Vou te entregar ainda mais! Na próxima aula teremos um guia, um passo a passo, pra te ajudar nas próximas etapas da sua carreira.

O que você precisa estudar, quais livros, o que seguir e mais.

@brunofraga.me

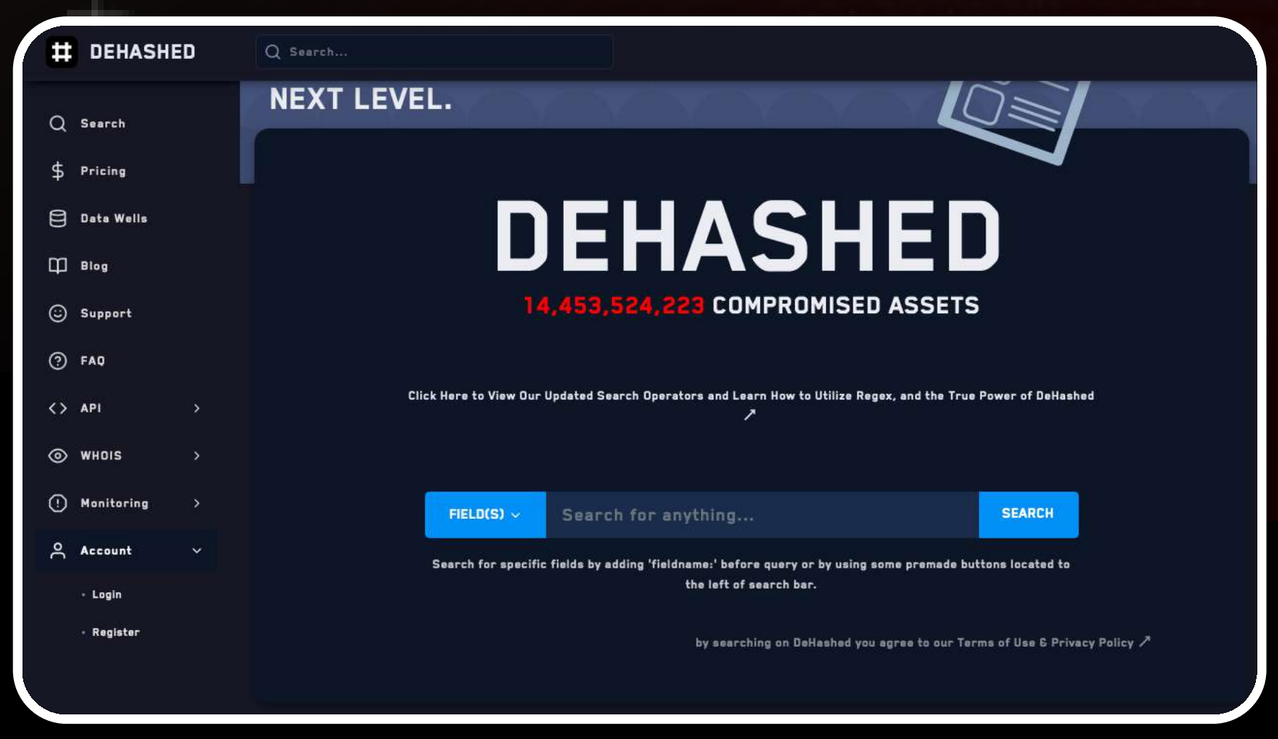
CAT RESULTADOS.TXT

DATA LEAKS

São os dados vazados. Você precisa mudar sua senha periodicamente, isolar senhas para contas diferentes.

Existe um mercado de dados vazados na Deep Web. As pessoas vendem e compram essas informações.

Eu utilizo um site (pago) chamado DeHashed: o site realiza **scans na Deep Web** e funciona como uma espécie de google de dados vazados.



VAZOU?

Como você pode verificar o vazamento de dados?

O site mais famoso e comum é o Have I Been Pwned.

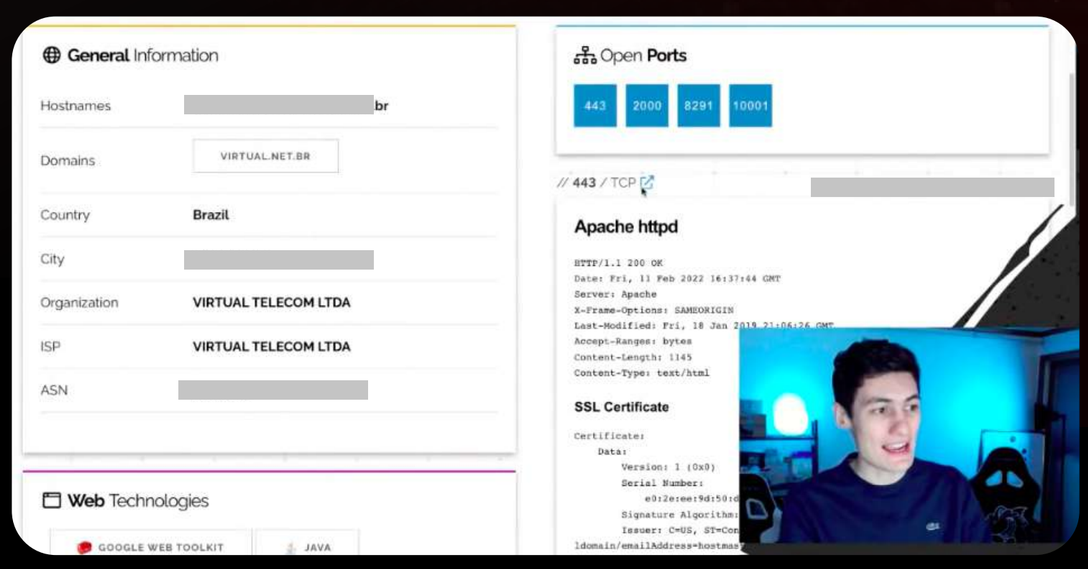
CAT RESULTADOS.TXT

GOOGLE DOS HACKERS

Focamos muito em google hacking, mas existe outra forma de buscar dados na internet.

Podemos buscar câmeras, geladeiras, webcams e diversos dispositivos com o Shodan.

No brasil conseguimos ter acesso a endereços IP vazados com ele, filtrar cidades, portas abertas, tipos de produto, etc.

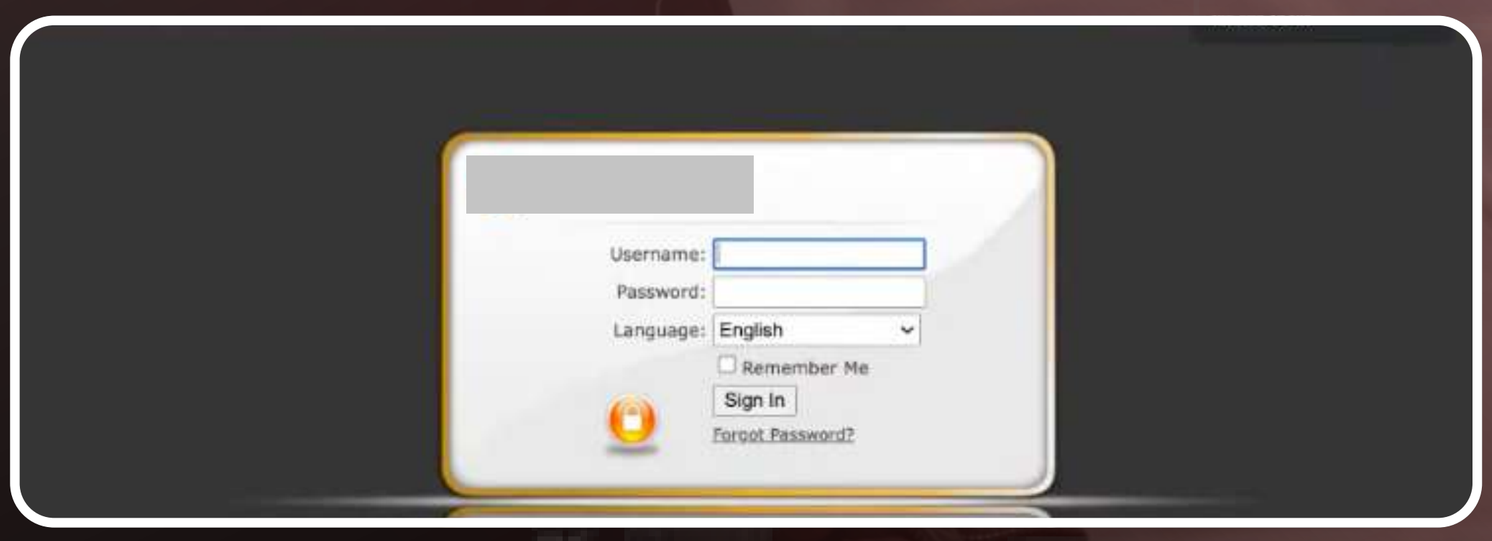


Aqui fomos capazes de encontrar um posto de gasolina público na internet. Isso significa que as informações do tanque desse posto estavam disponíveis

@brunofraga.me

CAT RESULTADOS.TXT

E assim fomos capazes de encontrar a interface da aplicação da bomba de gasolina



CAT SUBIR-DE-NIVEL.TXT

As inscrições abriram na aula 4! Vou te apresentar o Técnicas de Invasão e o desconto.

Além disso, você que se inscrever vai ganhar um bônus + a gravação da imersão.

Essa é a trilha definitiva de 6 passos pra você aprender hacking

@brunofraga.me

CAT SUBIR-DE-NIVEL.TXT

Uma das coisas mais importantes para os alunos e quem está começando é o Guia do Notion. Um guia de estudos, um template, pra te ajudar a aproveitar muito mais as aulas e o conhecimento adquirido.

É um conteúdo guiado, ou seja, você saberá o que estudar em cada um dos dias.

TOCA DO COELHO

Passo 1 → O livro do TDI
Passo 2 → Navegando no livro
Passo 3 → Sua base inicial
Passo 4 → Web hacking
Passo 5 → Hacking em Redes, IoT e Dispositivos
Passo 6 → O hacker ético

Acesso vitalício!

Bônus: Workshop hacker investigador + Guia de estudos no Notion + Comunidade do TDI no Discord

O certificado tem validade em todo território nacional, é válido como hora complementar também.

GARANTA SUA VAGA NO TREINAMENTO COM UM DESCONTO EXCLUSIVO DE R$400! USE O LINK:

👉 **ALUNOTDI.COM**

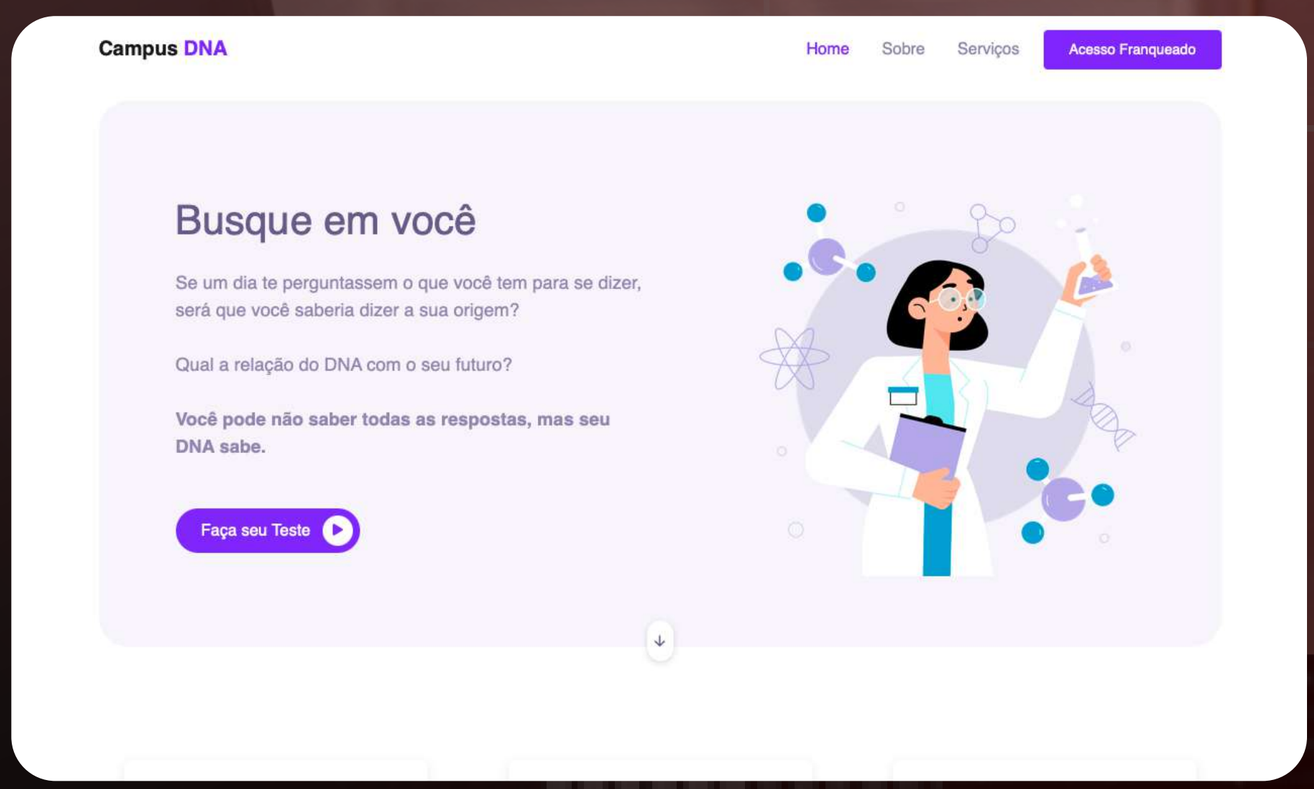
@brunofraga.me

CAT 0-ATAQUE.TXT

Como vai funcionar o ataque?

Vamos hackear um sistema juntos e entender todo processo passo a passo.

Nosso alvo hoje é uma empresa que lida com DNAs



PRIMEIRA ETAPA

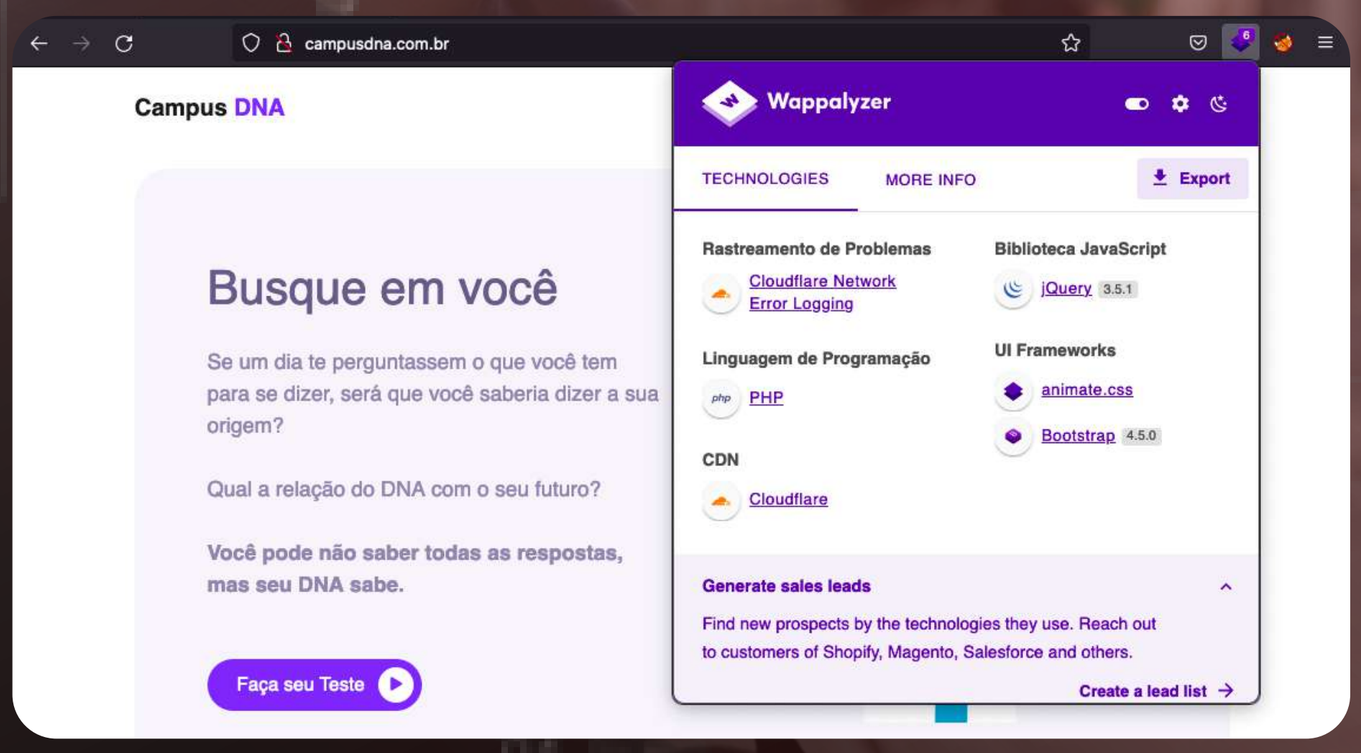
Primeira etapa do ataque hacker — o que devemos fazer? Conhecer, o nosso reconhecimento ou recon.

Vamos conhecer nosso alvo.

Podemos coletar imagens, observar os dados que são passados no site: eles possuem uma franquia? Existe informação de contato? Em um pentest podemos fazer um ataque de engenharia social.

CAT 0-ATAQUE.TXT

Com o Wappalyzer conseguimos mais informações da tecnologia do site:



PROXY

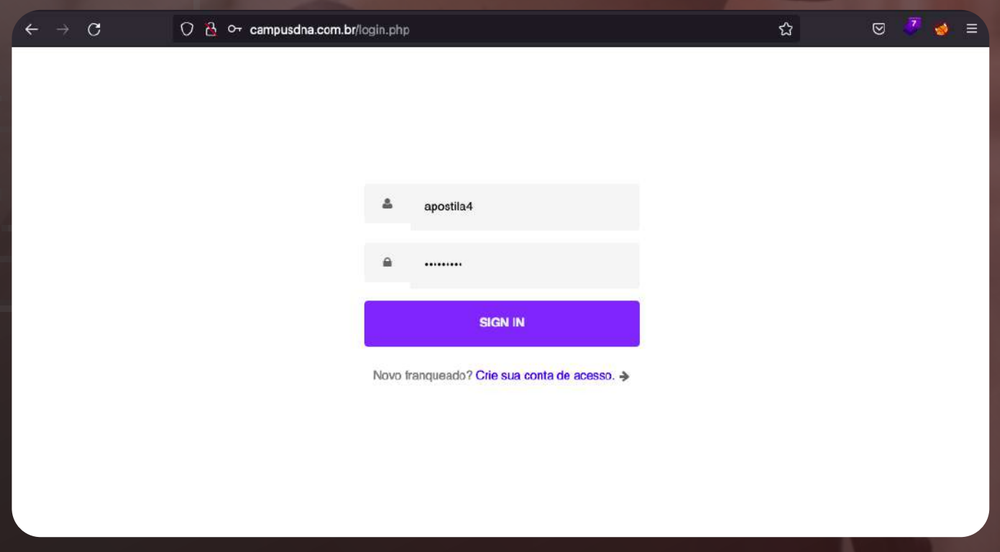
Descobrimos também dois painéis — um de login e outro de cadastro. Será que conseguimos colocar um email que não existe ou um usuário que não existe? São testes.

Vamos usar o Burp Suite — que é um proxy e serve como uma espécie de intermediário pra gente congelar e editar requisições web.

Também podemos ver o histórico do site, o sitemap: esse sitemap mostra toda a árvore de diretórios de um site, inclusive os que não conseguimos acessar normalmente pelo navegador.

CAT 0-ATAQUE.TXT

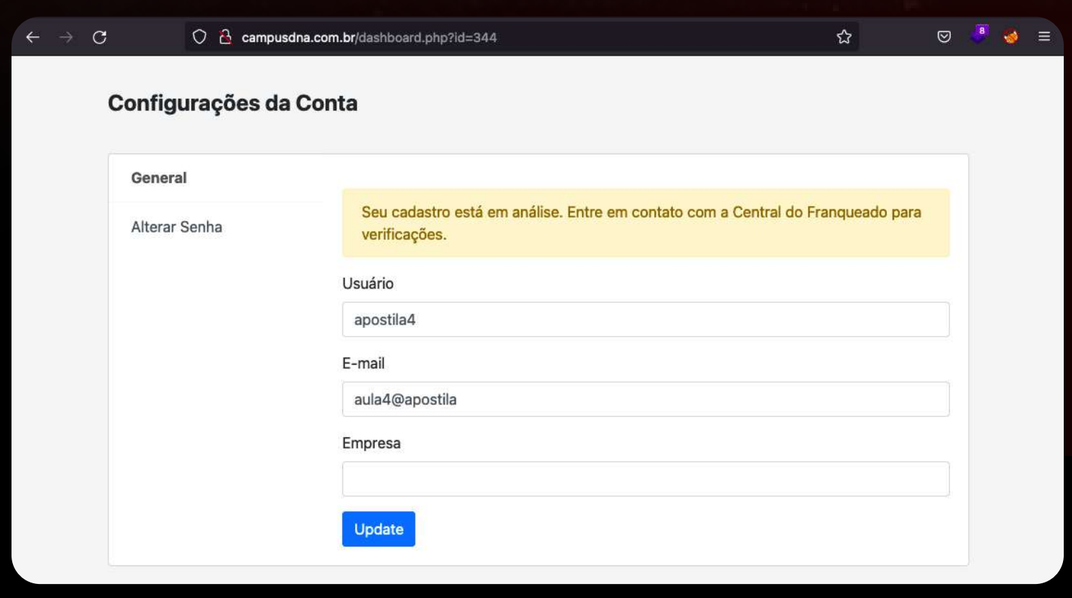
Vamos fazer nosso cadastro e login



Duas coisas aqui nos chamam a atenção: o endereço da URL e a informação de análise do cadastro.

A informação mostra pra gente que não temos muitas permissões - nossa conta está limitada.

A URL indica que o objeto referenciado com o indicador ID está exposto e possivelmente não está seguro também.
Podemos fazer o teste com o Burp Suite!



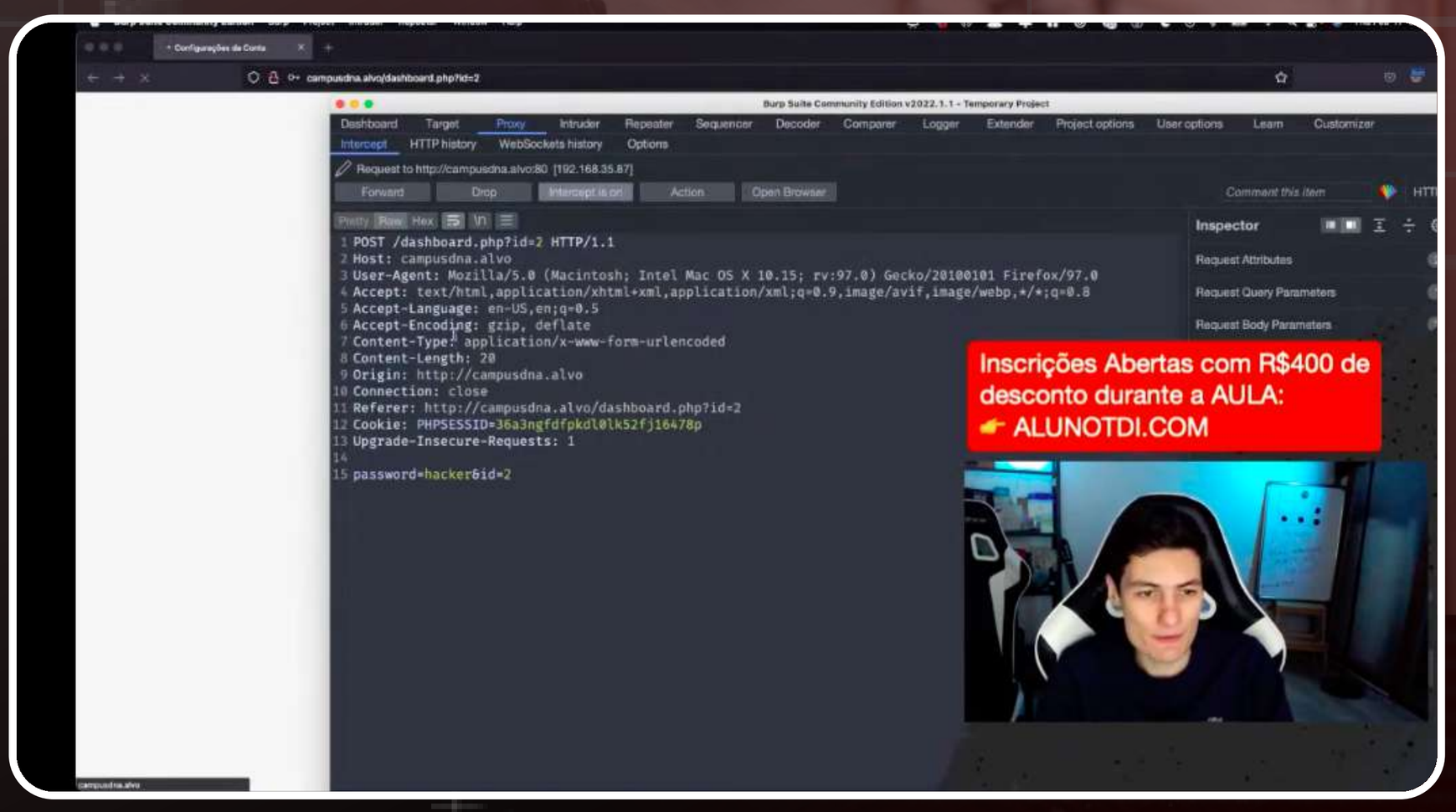
Mas antes, vamos listar as funcionalidades que podem ser analisadas ou exploradas no site:

➜ mudar a senha: como ele faz isso por de baixo dos panos?

@brunofraga.me

CAT 0-ATAQUE.TXT

Quando ligados o intercept do Burp e mudamos nossa senha no site, vemos que ele registra a requisição e alteração de senha



Aqui percebemos que é enviado para o site uma requisição com método POST e os parâmetros password e id.

O que acontece se mudarmos esses valores? Temos uma falha do tipo IDOR.

@brunofraga.me

CAT O-ATAQUE.TXT

INSECURE DIRECT OBJECT REFERENCE

O que é a falha IDOR? Na hackerone, ela tem um crescimento absurdo e é amplamente explorada.

Toda ação do sistema faz referência a um ID de usuário que não está isolado.

Por exemplo: pedido de iFood 123. Podemos alterar o pedido 123 para 1234 e obter outro pedido porque o programador não isolou e configurou da forma correta para um único usuário esse id.

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://campusdna.alvo
Connection: close
Referer: http://campusdna.alvo/dashboard.php?id=2
Cookie: PHPSESSID=36a3ngfdfpkdl0lk52fj16478p
Upgrade-Insecure-Requests: 1

password=hacker6id=1
```

Vamos mudar esse id para 1 e ver o que acontece: geralmente esse é o id do administrador.

GOOGLE HACKING

Vamos descobrir os nomes de usuários com recon para saber qual a relação dos IDs com google hacking

No processo de recon podemos fazer um bruteforce, banner grabbing, engenharia social...tudo o que for necessário para descobrir possíveis nomes de usuários.

@brunofraga.me

CAT 0-ATAQUE.TXT

Encontramos um board do Trello com informações sensíveis de administrador.

Já tinhamos a senha trocada, agora com o nome de usuário, ao tentarmos realizar o login, conseguimos acesso administrador na aplicação.

EXPLORANDO FUNCIONALIDADES

Podemos explorar outras coisas com o acesso de administrador: temos uma área de upload! Mais uma funcionalidade para ser explorada.

Conseguimos upar um arquivo malicioso? Conseguir uma shell?

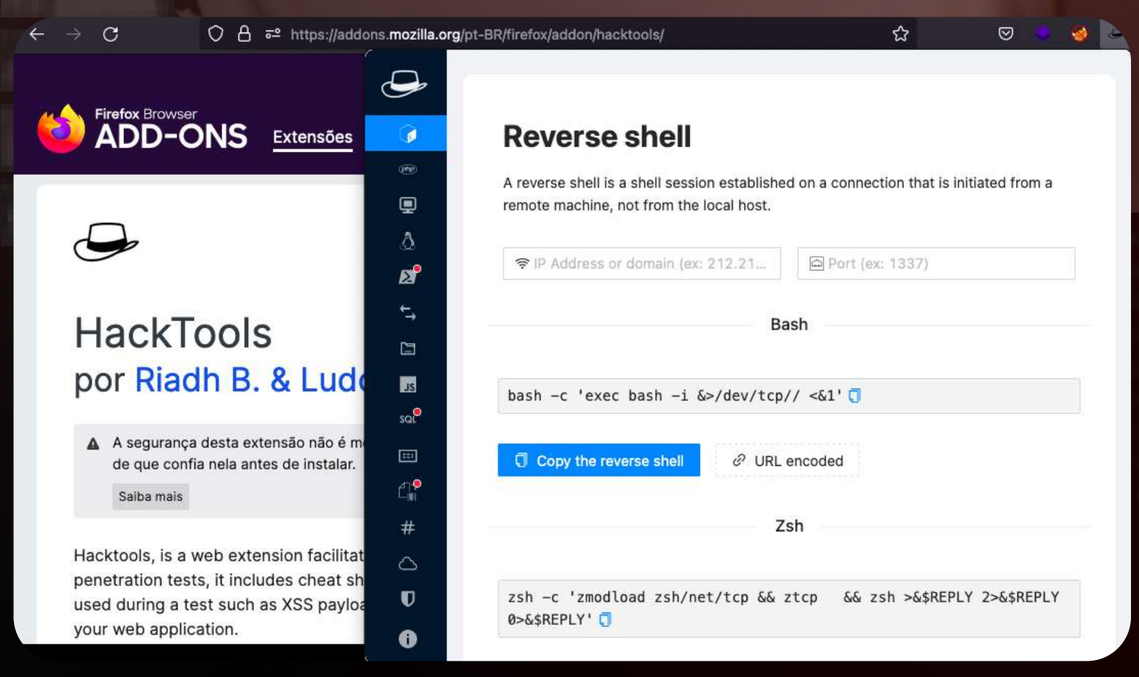
Vamos upar um arquivo malicioso que, se corretamente executado pelo site, conseguimos abrir uma porta!

CAT 0-ATAQUE.TXT

SHELL REVERSO

Podemos usar uma extensão chamada HackTools para usar nossa Reverse Shell.

É um shell reverso porque conectamos isso do alvo para o atacante e não do atacante para o alvo. Por isso é chamada reverse, já que faz um processo reverso.



Em nossa máquina local podemos usar o Netcat para abrir uma porta em nosso pc para escuta. É com ela que conseguiremos acesso a uma shell no alvo,

```
nc -lnv 3000
```

Com o nosso ip e porta selecionados, podemos montar nossa reverse shell. Essa extensão monta um código em PHP pra gente (sabemos que nossa aplicação usa php).

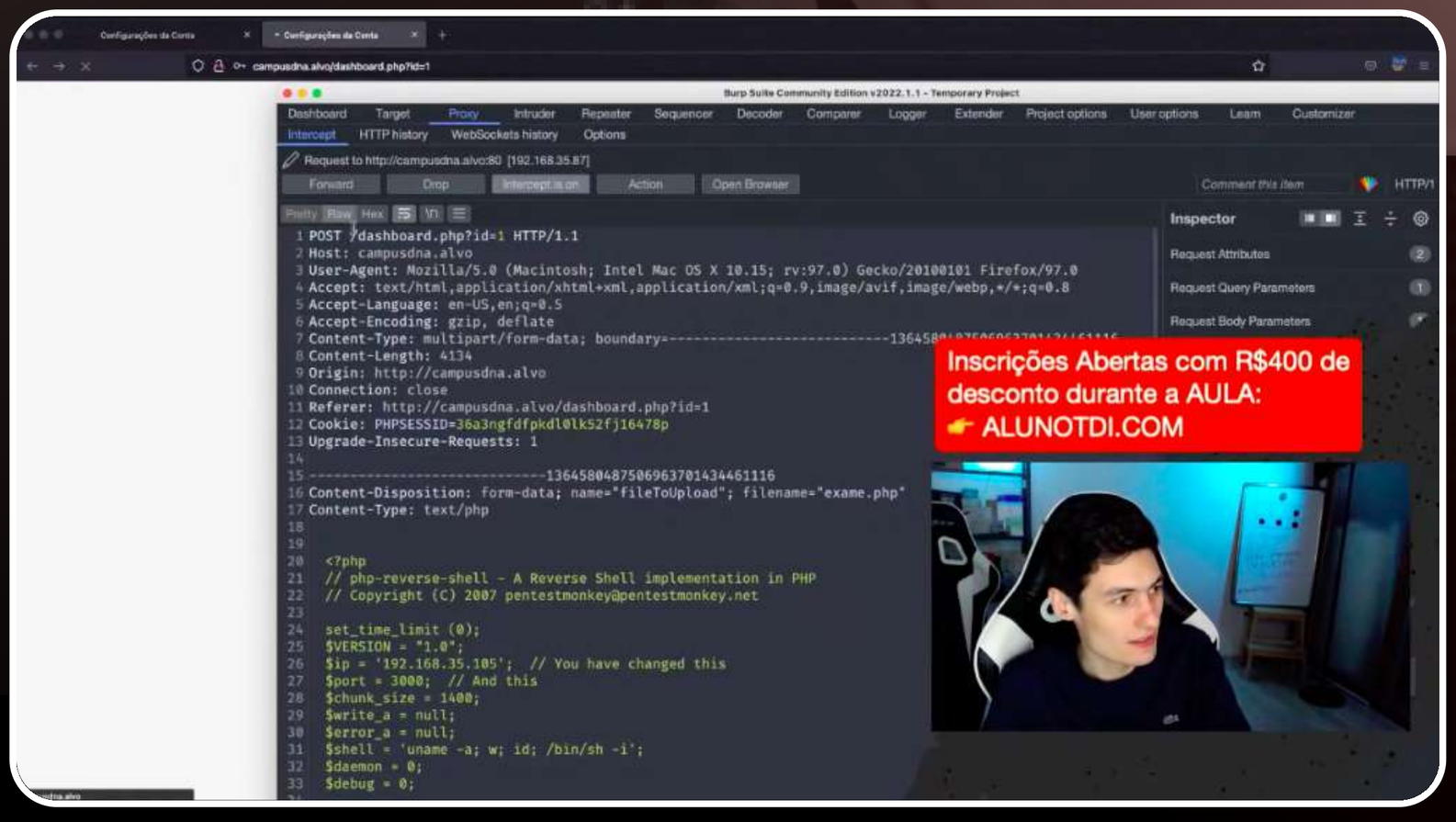
CAT 0-ATAQUE.TXT

REVERSE SHELL CHEAT SHEET

Esse processo de shell reverso e seus códigos podem ser encontrados na internet com um cheat sheet — uma tabela com diversos códigos maliciosos.

Agora vamos criar nosso arquivo pra ser upado.

Aqui com o Burp podemos interceptar e registrar a requisição pra análise.



Feito o upload vimos que há um problema!

Não deu certo. Nosso alvo não deixa a gente inserir um arquivo PHP.

@brunofraga.me

CAT 0-ATAQUE.TXT

BYPASS

Podemos testar extensões diferentes? Vamos pensar na **lógica de programação**: como ele está cancelando as extensões? Isso depende da regra do programador.

Se ele delimita upar somente .png e usarmos uma extensão shell.png.php então nós podemos fazer o upload.

Agora se na lógica ele deixa explicito não permitir extensões que ACABEM com .php a coisa muda.

INTRUDER

Podemos usar o Burp pra automatizar nosso processo com o intruder, usando wordlists para quebrar a lógica do programador.

Arquivos PHP possuem diversas extensões e a filtragem é algo sensível e perigoso porque muitas pessoas fazem isso de forma errada.

@brunofraga.me

CAT 0-ATAQUE.TXT

Vamos mudar nosso arquivo para .phtml em uma tentativa e assim conseguimos realizar o upload com sucesso!

Quando executamos o arquivo, a requisição chega para a nossa máquina e conseguimos acesso ao servidor, mas sem muita permissão, estamos como www-data.

ESCALANDO PRIVILÉGIOS

Descobrimos que o usuário John tem acesso a um binário chamado toto que possui permissões suid.

A escalação de privilégios é uma outra etapa do hacking! Isso está totalmente ligado à permissões do linux.

No linux quando executamos um arquivo, temos algo chamado path.

CAT 0-ATAQUE.TXT

ENVENENAMENTO DE PATH

O comando **echo $PATH** retorna uma informação do caminho pra gente. Com isso, podemos fazer um processo de envenenamento de PATH.

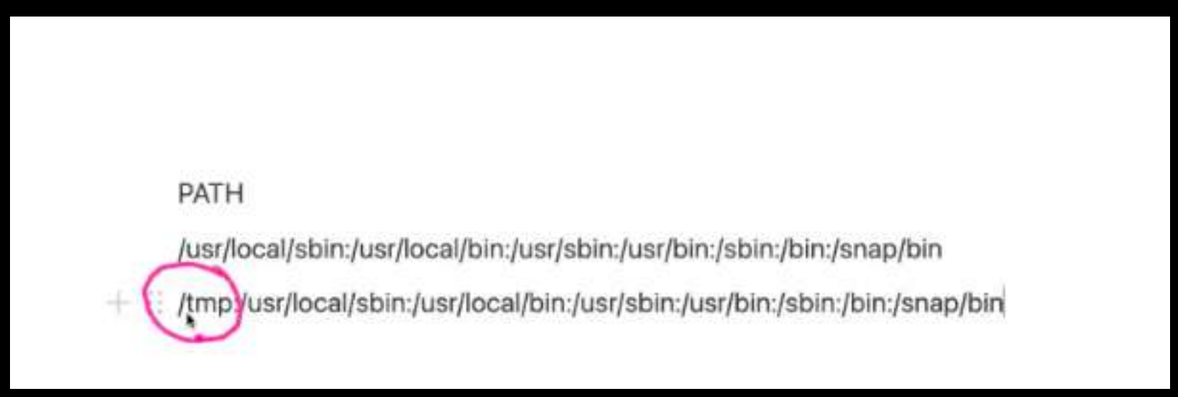
Vamos tentar trocar o path do binário para conseguir uma shell como john.

Como fazemos isso?

```
echo 'bash' > /tmp/id; chmod +x /tmp/id
# tmp eh temporario e todos conseguem escrever nele

Vamos sobrescrever essa PATH agora

export PATH=/tmp:$PATH
```



Quando o linux for executar o id ele ignora o restante do local e considera a informação /tmp

e executando o arquivo **./toto** novamente conseguimos um bash como john.

@brunofraga.me

CAT 0-ATAQUE.TXT

Podemos listar arquivos e procurar alguma senha do usuário john.

Através de um dos arquivos de backup, conseguimos uma senha.

Vamos usar o ssh com as credenciais do john no campusdna.alvo

ACESSO ROOT

o John ainda não é o root. Por isso vamos escalar privilégios dele para o root.

O que o John consegue executar? Podemos descobrir com o comando **sudo -l**.

Assim descobrimos que ele consegue executar como root o python3.

Em python, sabemos que o os.system() é um recurso interessante para ser usado num cenário de ataque: ele funciona como uma forma de executar comandos no sistema através da linguagem.

CAT 0-ATAQUE.TXT

Aqui podemos envenenar o comando /home/John/file.py com o os.system para rodar com root.

```
echo "import os; os.system('bin/bash')" > /home/john/file.py

## Vamos usar a permissão de sudo para executar o python3

sudo /usr/bin/python3 /home/john/file.py

> whoami
> root
```

Conseguimos acesso root ao sistema!

Essa é a essência da escalação de privilégios.

A partir daqui, podemos decidir o que fazer com esse acesso.

Isso vai da criatividade e dos objetivos do hacker.

@brunofraga.me

CAT AULA-5.TXT

Nossa última aula está chegando!

Nela você vai receber um guia completo, um passo a passo, o seu norte para continuar sua jornada de estudos de hacking em 2022!

Vou te mostrar tudo o que você precisa para ir além no mercado de Segurança da Informação.

Se você quer trabalhar ou se tornar um hacker profissional: essa aula é pra você.

CAT LEGIAO.TXT

Não esqueça de compartilhar conosco seus estudos no instagram com a hashtag #HackingEm2022

@planohacking

INTENSIVÃO

HACKER PROFISSIONAL

TÉCNICAS DE INVASÃO