

SEMANA DO
HACKING

***COMO HACKEAR
UM SISTEMA***



CAMPO DE BATALHA

OVERVIEW

Falaremos sobre

- Nossos alvos
- Hacking em aplicações web
- Ferramentas
- Técnicas de exploração

DICAS

A Semana do Hacking está servindo como um Guia de Estudo prático. Portanto, não seja um aluno passivo!

Escreva comandos, crie tópicos, faça o que precisa para estudar ativamente e tirar o máximo de proveito.

INVADINDO MÁQUINAS

Vou te fazer uma provocação...O que você almeja como estudante de hacking?

1. Passar 05 anos estudando livros e mais livros para somente depois começar a hackear;
2. Colocar o que você já está aprendendo em prática - HOJE - e partir para o campo de batalha;

PORTAS ABERTAS

Se escolheu a segunda opção, então você tem o que precisa para fazer parte da Legião de hackers éticos do TDI.

Aqui, vamos te dar a chance de ver esse mundo com novos olhos (você escolheu a pílula vermelha!), conhecer uma metodologia que vai transformar sua forma de hackear sistemas e, quem sabe, entrar na toca do coelho.

Aceita o desafio?

CAMPO DE BATALHA

PODERES

Com grandes poderes vem grandes responsabilidades. Você já ouviu essa frase do Tio Ben, certo!?

Por isso, o primeiro passo é entender como o atacante age. Essa é a melhor forma de aprender!

É isso que acontece no mundo hacker. Você tem habilidades e um grande poder em suas mãos, capaz de transformar ou destruir.

É preciso conhecer seu inimigo.

Aqui, nosso objetivo é único, formar uma legião de hackers éticos.

“A habilidade de alcançar a vitória mudando e adaptando-se de acordo com o inimigo é chamado genialidade”

Sun Tzu em A arte da Guerra

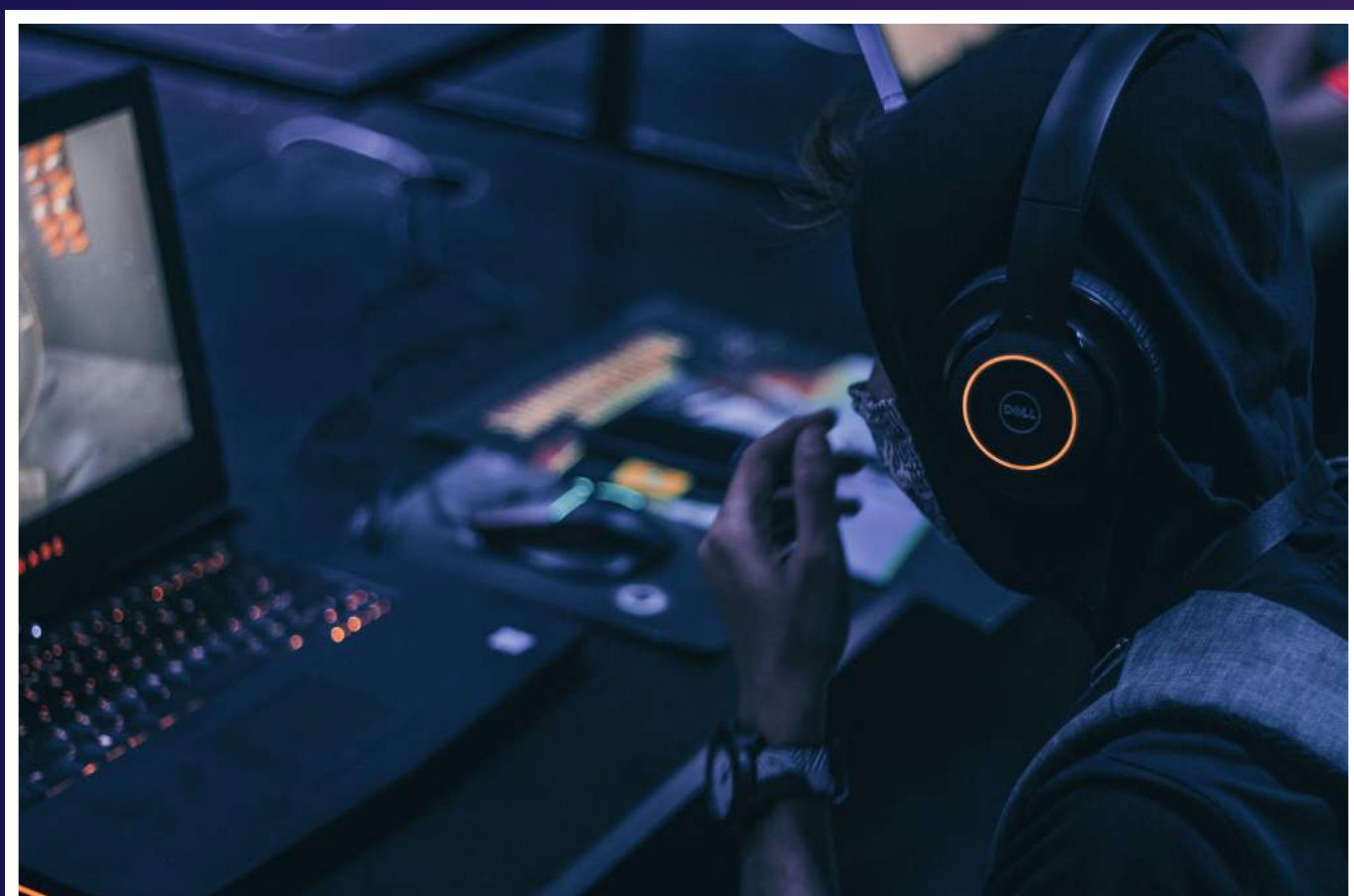
CAMPO DE BATALHA

NOSSO ALVO

Dentro de um pentest temos duas possibilidades:

1. Ataque black box ou caixa preta: você tem pouquíssima ou nenhuma informação do alvo. Precisa correr atrás!
2. Ataque white box ou caixa branca: É acertado um escopo com informações de endereços ips e alvos que farão parte do ataque.

No nosso caso, temos a informação do site alvo que será hackeado.



HACKEANDO APLICAÇÕES WEB

A primeira e mais importante etapa do nosso ataque é conhecida como RECON ou Reconhecimento: aqui vamos descobrir e conhecer tudo o que estiver disponível sobre o nosso alvo.

Empresas não usam somente o site principal. Muitas possuem blog, intranet, painel de login, VPN, acesso remoto, sistema interno, CRM e por aí vai!

OLHANDO PARA O OUTRO LADO

A maioria dos hackers não focam muito no site principal e sim nas outras aplicações, que muitas vezes não são feitas para o público.

CAMPO DE BATALHA

ESCOPO

Para aumentar nosso escopo vamos focar em encontrar outras aplicações descobrindo subdomínios.

Aqui, podemos usar o subfinder para enumerar subdomínios.

Uma das grandes vantagens no hacking é sermos bons em recon e sabermos coletar informações do nosso alvo.

Então, sempre pratique isso!

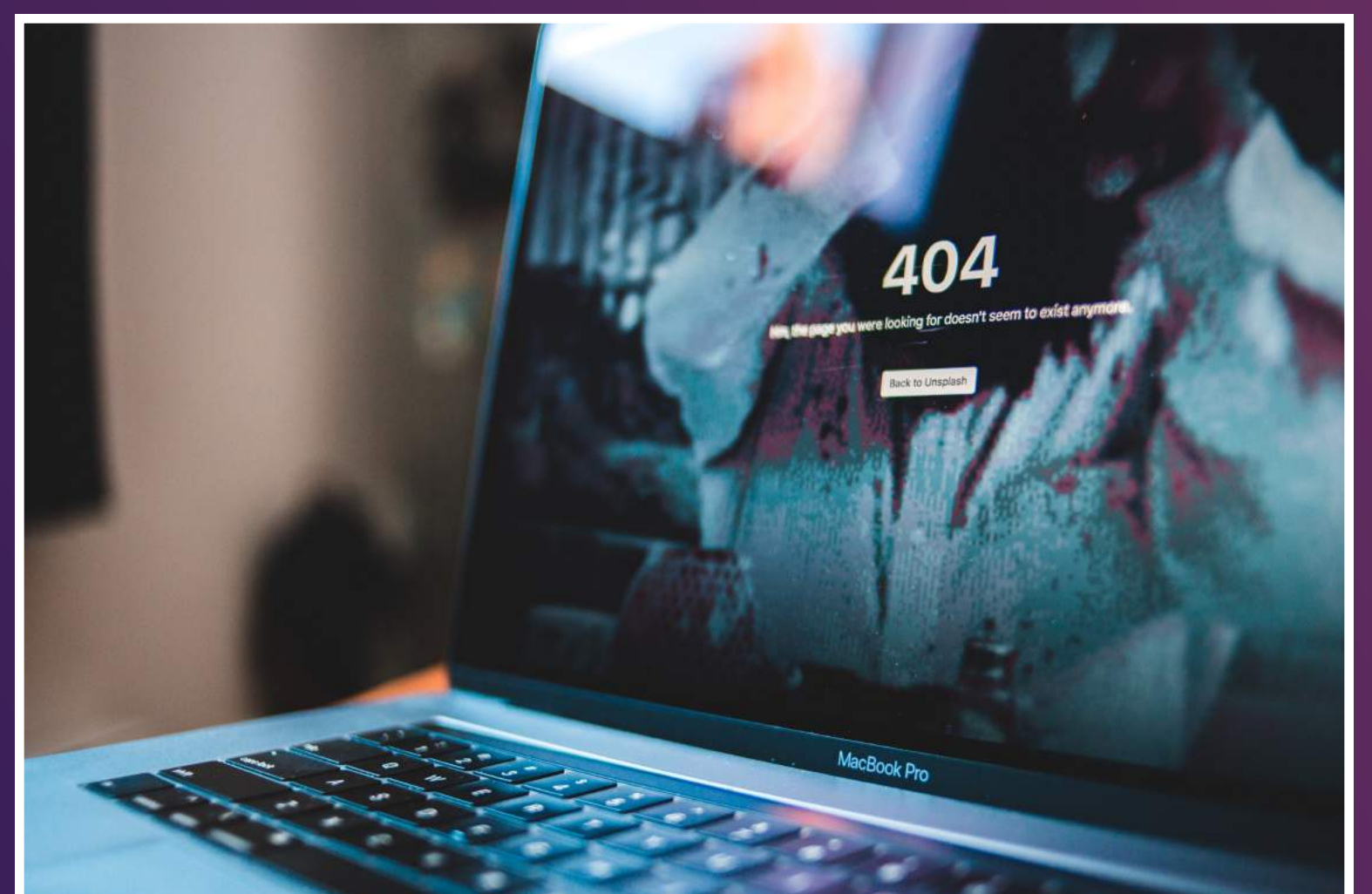
Aqui também a ideia é gerar erros:

- Clique em tudo o que puder
- Veja sempre o código fonte
- Clique em sobre para obter informações
- Liste diretórios da aplicação

GERE ERROS

Diferente de usuários comuns, hackers prestam atenção nos mínimos detalhes.

Por isso, se um erro aparece, lemos as mensagens de erro do sistema/aplicação.



CAMPO DE BATALHA

APLICAÇÕES WEB

Um dos grandes problemas das aplicações web é confiar demais nos usuários, não existe um controle ou sistema de validação rigoroso, então podemos explorar isso!

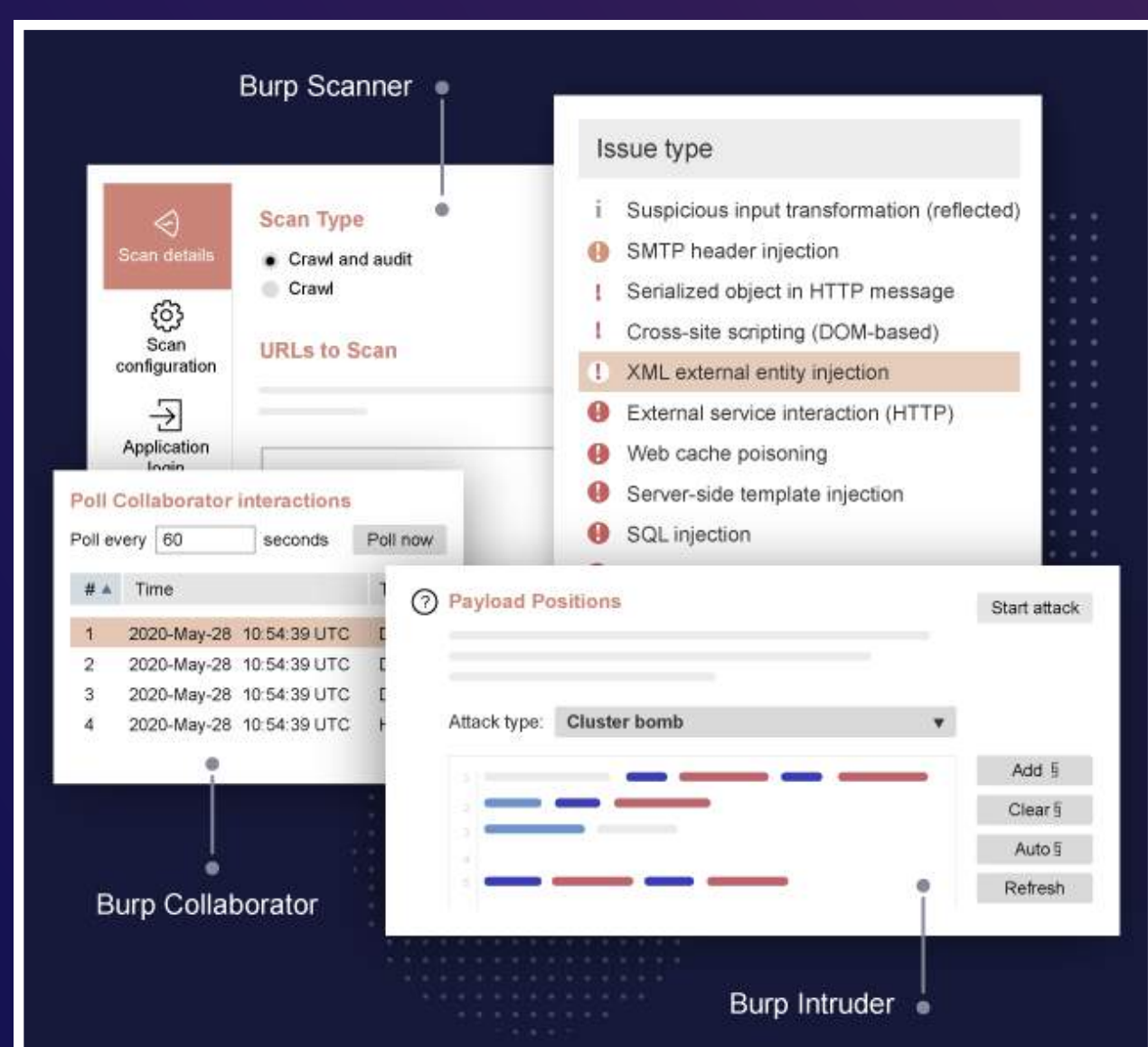
Em um sistema web, enviamos uma solicitação e recebemos uma resposta. Isso significa que podemos, dentro de um site, utilizar o DevTools para inspecionar as requisições e analisá-las.

FERRAMENTAS

Outra ferramenta de extrema utilidade é o Burp Suite. Ele servirá como um proxy, um intermediário, entre você e a aplicação.

Aqui teremos a liberdade de interceptar, modificar e realizar novas requisições.

O Hacktool também é uma ferramenta útil para aplicações web: uma extensão do navegador que nos auxilia com diferentes possibilidades de testes e injeções, funcionando como um canivete suíço.



..... Burp Suite
Community Edition

WRITE-UP

01 ETAPA - ENUMERAÇÃO

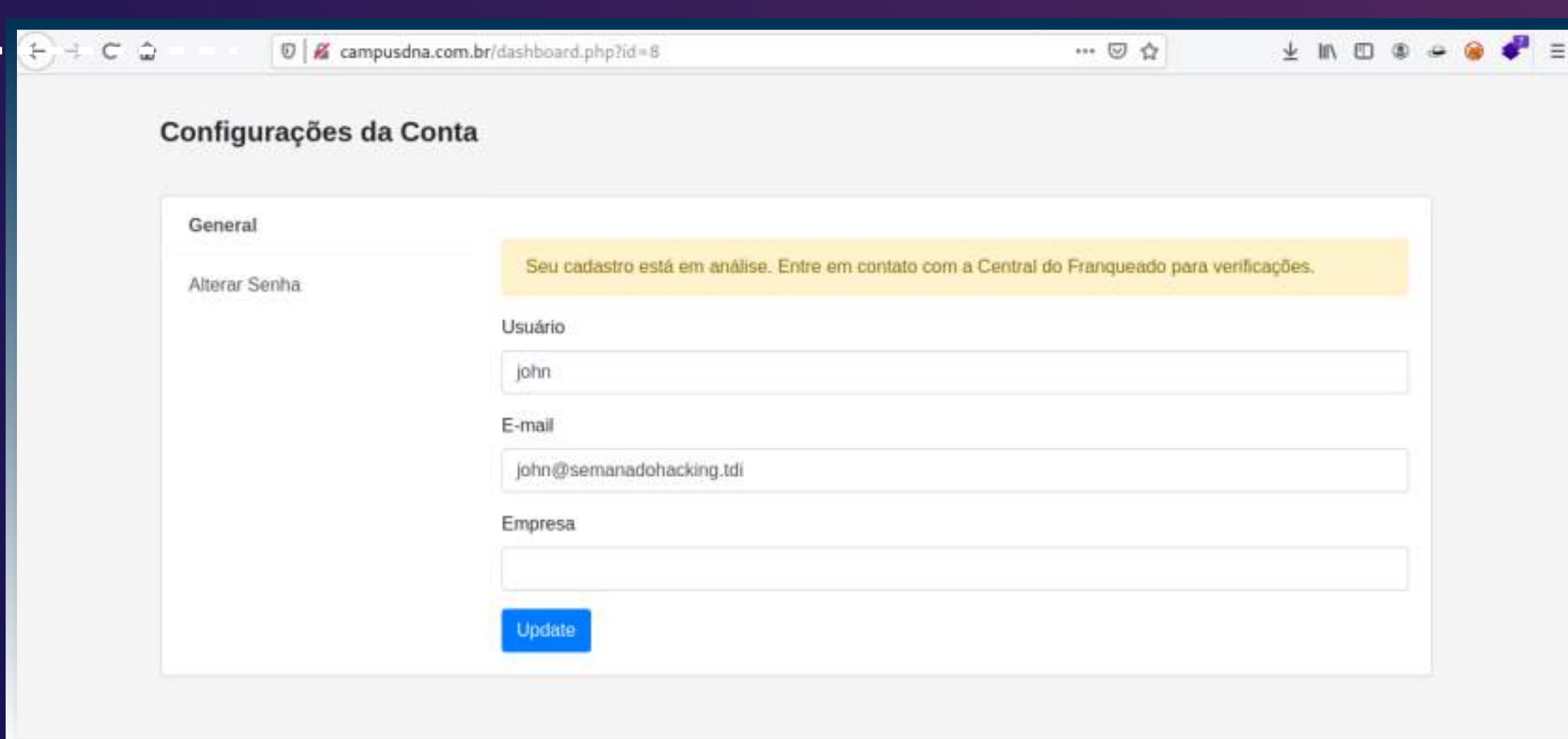
Iremos acessar o site alvo, vamos analisar a aplicação web afim de encontrarmos uma página de login, por exemplo.

Podemos tentar enumerar usuários registrados no sistema. Temos uma conta admin existente ou root?

02 ETAPA - LEVANTAMENTO E ANÁLISE


Depois que o proceso de enumeração acaba (e esgotamos nossas tentativas), é preciso levantar as possíveis vulnerabilidades.

O que aquele site pode conter: Um SQL Injection? Fazemos os testes nos inputs de login. Um IDOR? Verificamos a URL da aplicação ao realizarmos o login.



Nessa etapa é importante termos conhecimento dos tipos de vulnerabilidades web. A OWASP pode nos ajudar com isso.

Ao tentarmos trocar o ID para 1 e visualizar os dados do admin, somos bloqueados pela aplicação com a mensagem “Your not allowed to access another user information”. Isso mostra que algo no back-end está nos bloqueando.

 |  campusdna.com.br/dashboard.php?id=8

WRITE-UP

03 ETAPA - ENUMERAÇÃO PARTE 2

Vamos tentar descobrir, através da enumeração, o que está acontecendo por trás do site. Pra isso, utilizaremos o Burp Suite.

Aqui interceptaremos como os dados são enviados, descobrindo que o site está vulnerável a Account Takeover.

Isso significa que podemos trocar a senha de outro usuário pela nossa própria conta, através do recurso “alterar senha”.

Isso significa que o usuário não está sendo validado para realizar essa ação!

04 ETAPA - EXPLORAÇÃO

Para explorarmos o Account Takeover, precisamos interceptar a requisição de troca de senha com o Burp Suite.

Assim, trocamos os valores dessas variáveis antes de enviar para o sistema.

Na aplicação, sabemos que o id do administrador é 1.

Assim, inserimos esse id (id=1) e alteramos a senha do usuário.

```
password=senhateste&id=1
```

Em seguida, ao tentarmos realizar o login com o user admin, conseguimos acesso administrador na aplicação.

WRITE-UP

05 ETAPA - FILE UPLOAD

Analizando a dashboard do administrador, descobrimos que é possível upar arquivos na aplicação.

Se podemos fazer o upload de um arquivo, isso significa que podemos tentar upar algo malicioso...certo?

Como desejamos acesso root ao sistema, vamos tentar upar um shell reverso através do file upload.

O problema é...ele restringe o upload de arquivos a alguns tipos específicos.

Como iremos contornar isso?

-> BYPASS

Podemos contornar, ou seja, realizar um bypass na aplicação.

Isso significa que vamos enganar o sistema, fazendo ele pensar que estamos upando um tipo de extensão, quando na verdade está upando outra.

E aqui entra uma etapa importante: através do terminal, abrimos uma escuta para a porta configurada no shell reverso (o código maliciosos que enviaremos pra aplicação).

Podemos fazer isso com o Netcat, através do comando: `nc -lnvp porta`.

WRITE-UP

06 ETAPA - I'M IN!

Conseguimos uma shell como www-data no sistema.

Vamos aproveitar para listar diretórios e verificar permissões.

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

Vamos envenenar, ou seja, tentar trocar o path do binário para id para conseguir uma shell como john.

```
echo 'bash' > /tmp/id; chmod +x /tmp/id; export PATH=/tmp:$PATH
```

Executando novamente o ./toto teremos uma shell como John.

07 ETAPA - ESCALANDO PRIVILÉGIOS

Agora que estamos como john, vamos listar os arquivos contidos na máquina através do comando: ls -la

Através do arquivo .backup_password descobrimos uma senha root123.

Vamos usar o ssh: ssh john@ipdamaquina

Aqui podemos nos perguntar: o que o John tem permissão de executar?

Descobrimos através da análise do sudo -l que o mesmo pode executar um arquivo python sem senha.

Podemos inserir nossa payload dentro desse arquivo e pegar shell como root!

WRITE-UP

08 ETAPA - I AM ROOT!

Em Python, existe uma função chamada `os.system()` que nos permite executarmos comandos no sistema.

Usaremos nossa payload desta forma:

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

RATO OU HACKER?

Quando escalamos privilégios, fazemos isso como um rato, procurando diversos caminhos e possibilidades.

Por isso, é importante entendermos bem o funcionamento do sistema!

Finalmente, conseguimos acesso root ao sistema!

Agora podemos desfrutar de todas as liberdades de permissão e usar nossa criatividade: vamos exfiltrar dados? instalar um malware ou backdoor?

O repositório GTF0Bins, no GitHub, nos auxilia com diversos comandos para escalarmos privilégios.



SHELL REVERSO

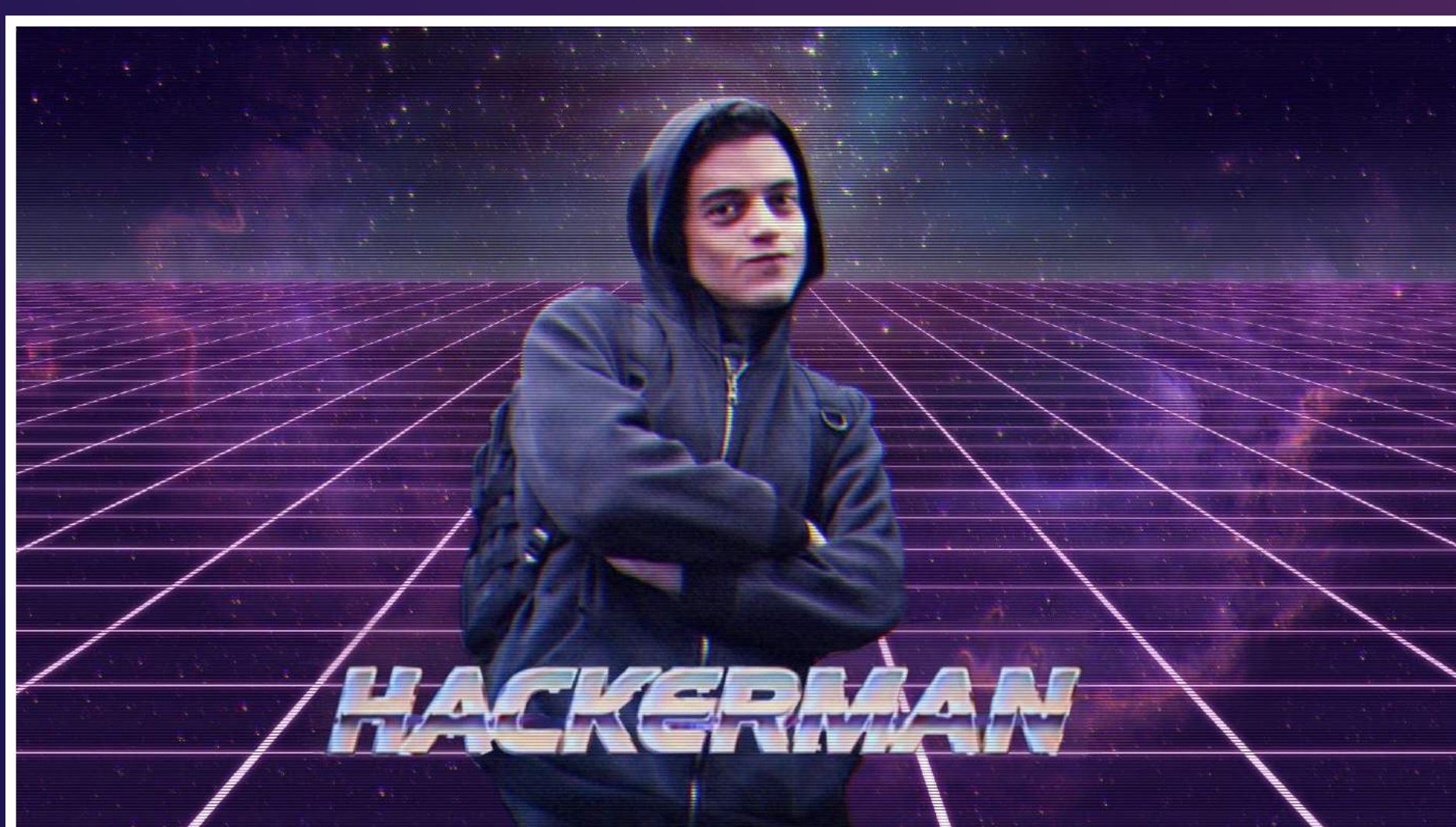
IP PRIVADO E PÚBLICO

É importante dizer que, no processo de invasão, abrir uma porta no roteador expondo seu IP não é legal.

Por isso, utilizamos o Ngrok que nos permite subir um serviço web.

Esse IP sim se tornará público, mas será de uma aplicação externa, impedindo que sejamos expostos sem necessidade.

Basta configurarmos o IP e portas e escutarmos com o netcat para realizar o mesmo processo que faríamos em nossa máquina local.



Lembre-se da importância de estudar programação, conceitos de shell, conexão remota e escalação de privilégios.

A PÍLULA

DOSE DE HOJE

Agora me diz...depois dessa experiência prática, você quer voltar para os livros empoeirados ou ir além?

No TDI, estamos sempre buscando te levar ao próximo passo - **HACKEANDO NA PRÁTICA.**

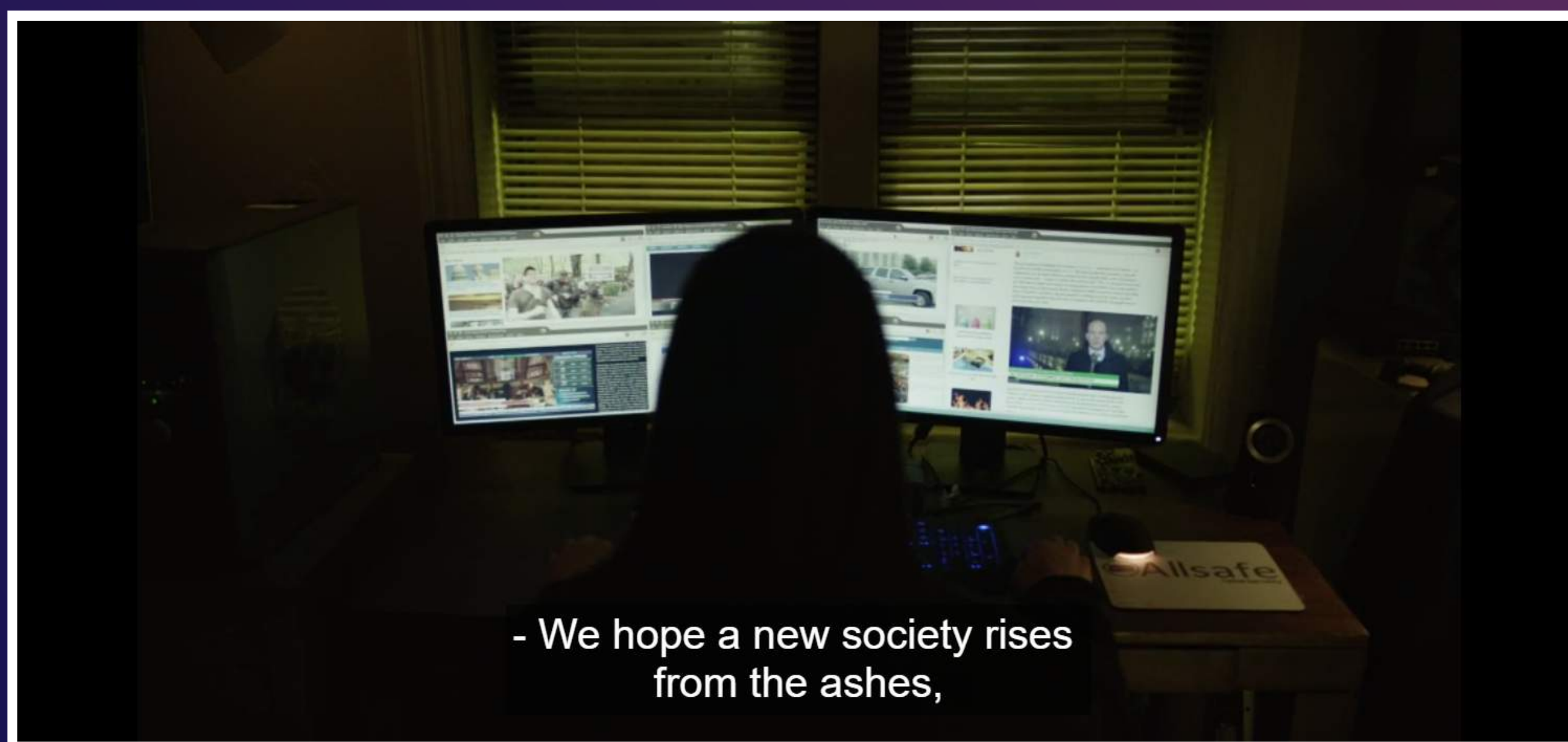
Por isso, vou mostrar o que te aguarda na próxima live....

ENTRANDO NA TOCA

- Você vai conhecer a trilha
- Vou te explicar qual é a melhor linguagem e quais os sistemas usados por hackers do mundo inteiro!

Farei uma live de mentoria. Um encontro, ao vivo, feito especialmente para ajudar os estudantes.

Você poderá tirar todas as suas dúvidas!



- We hope a new society rises
from the ashes,

Diz aí...não dá pra ficar de fora, não é mesmo? Espero você do outro lado!



"My crime is that of curiosity"