

# INTRODUÇÃO AO HACKING



[guiahacker.com](http://guiahacker.com)

# SOBRE O AUTOR

M.Barreto - O Guia Hacker

Olá caro leitor, tudo bom?

Meu nome é Matheus, sou cientista da computação, trabalho com ethical hacking há 8 anos, e como programador há pelo menos 12.

Caso não saiba, eu sou o idealizador, criador e atual professor principal do treinamento **Guia Hacker**, um treinamento certificado em hacking, 100% prático em português. E agora também autor deste e-book 😊

Antes de continuar vou te convidar para visitar o site do **Guia Hacker**. Basta clicar aqui ou acessar o site: [guiahacker.com](http://guiahacker.com)

# O QUE É UM HACKER?



Hacker são indivíduos com grande conhecimento em computação, graças a isso são capazes de realizar modificações e ataques em sistemas pré-estabelecidos.

Os Hackers são ótimos analistas, capazes de desvendar falhas através de técnicas "secretas e obscuras", do mundo da computação.

**Obs.:** Muitos confundem os termos "hacker" e "cracker".

*Abordaremos na próxima página.*

# HACKERS SÃO CRIMINOSOS?

Definitivamente **NÃO**.



Essa questão é uma má fama propagada pela mídia. Na realidade **hackers** utilizam seus conhecimentos em prol de defender sistemas, ou localizar brechas para que sejam corrigidas. Um ethical hacking ganha dinheiro encontrando falhas e às notificando para que sejam sanadas, sem prejudicar a terceiros.

Os verdadeiros criminosos são denominados de **Crackers**, estes utilizam o conhecimento para lesar terceiros.

# COMO HACKERS GANHAM DINHEIRO?

Talvez você já saiba, talvez não. Mas **ethical hacking** é uma das profissões mais valorizadas no mundo da tecnologia, e atualmente está em forte ascensão devido a novas leis, como a LGPD, que vem sendo criadas ao longo do tempo.

Imagine quanto um banco pagaria por informações de uma falha em seu sistema? Muito, acredite...

Hackers éticos, profissionais, chegam a faturar **R\$40.000,00** (quarenta mil reais), **por mês**.

# COMO POSSO ME TORNAR UM HACKER?

Muitos querem se tornar hackers profissionais, mas sinceramente e infelizmente, esse é um conteúdo extremamente escasso. Existe pouco conteúdo disponível por ai, e em português menos ainda.

Por conta disso estou fazendo esse e-book para te guiar, acredito que com isso você possa dar seus primeiros passos. E quem sabe em seguida subir de nível e entrar para o nosso clube do **GUIA HACKER**.

CLIQUE AQUI PARA  
ACESSAR O **GUIA HACKER**

# ENTENDENDO O BÁSICO

Vamos falar do mínimo que você **PRECISA!** conhecer, sobre computação para iniciar no mundo do **hacking**.

Nas próximas páginas você vai ingressar no mundo avançado da computação.

Lembre-se:

***só quem persiste alcança!***

# O HARDWARE

Definição: Parte física do computador basicamente é tudo aquilo que você consegue pegar e chutar.

Ex.: Placa mãe, processador, memória ram, hd, etc...

Vamos falar sobre:

- Placa mãe
- Processador
- Memória RAM
- Placa gráfica



# PLACA MÃE

Peça responsável por conectar todos os outros componentes do sistema computacional.

A placa mãe precisa conter slots(encaixes) para o processador, memórias ram, discos rígidos (hds), placas gráficas, placas de áudio, e outros dispositivos que por ventura venham a ser desenvolvidos.

# PLACA MÃE

Mas não é somente conectar os dispositivos a responsabilidade da placa mãe.

Este incrível dispositivo é responsável por sincronizar todos estes componentes para que eles possam conversar entre si, através do mesmo barramento de dados.

# PLACA MÃE BARRAMENTO

O Barramento consiste em conexões na placa mãe, que são responsáveis por passar informações de um componente para o outro.

Porém diversos componentes usam o mesmo barramento, por conta disso eles não podem enviar e receber informações ao mesmo tempo.

Quando um componente usa o barramento para escrever, os outros componentes devem ficar somente escutando.

# PLACA MÃE BARRAMENTO

Quem faz este controle, chamado de sincronização. São alguns subcomponentes presentes na placa mãe, conhecidos como "ponte norte" e "ponte sul". Os quais são mais complexos e por isso deixo a explicação para os membros do **Guia Hacker**.

O importante é que você saiba que isso existe e é crucial para o funcionamento do computador.

# PROCESSADOR

O componente famosinho, e não é atoa. O processador é o cérebro do computador.

Este componente é o responsável por processar as entradas e os comandos programados pelo desenvolvedor para que seja possível realizar alguma ação no sistema computacional

# PROCESSADOR

O processador trabalha em conjunto com os outros dispositivos para entregar saídas para o usuário.

Seja exibir uma imagem, processar um cálculo ou rodar um game. Tudo passa por este carinha tão importante

# PROCESSADOR

Processadores possuem algumas características importantes, como a frequência, número de núcleos e quantidade de threads.

Vale ressaltar que já existiram diversos ataques hackers envolvendo a frequência do processador e até mesmo características internas recentes

# PROCESSADOR A FALHA DA INTEL

O Meltdown reverso é um problema descoberto, recentemente, nos processadores da Intel. Esta falha permite ao hacker acessar áreas sensíveis da memória do processador, onde informações importantes como senhas estão armazenadas temporariamente.

A Intel soltou uma atualização emergencial, que...



# **PROCESSADOR A FALHA DA INTEL**

A Intel soltou uma atualização emergencial, que inibe o ataque a esta falha, porém em contrapartida o processador perde 30% do seu poder de processamento.

Muitas pessoas não realizaram a atualização e seguem vulneráveis até hoje...

# MEMÓRIA RAM

Muitas vezes chamada apenas de memória, ou memória principal, este componente é o responsável por armazenar dados que necessitam de maior velocidade de acesso.

Ou seja, o conteúdo que estiver rodando atualmente, em outras palavras, sendo processado pelo processador, precisa estar em memória ram

# MEMÓRIA RAM

Casos onde é necessário rodar um programa maior do que a quantidade de memória.

Ex.: Um jogo de 40gb, para 8gb de ram.

É necessário utilizar técnicas de paginação, estas técnicas são aplicadas pelo próprio sistema operacional e pode apresentar vulnerabilidades interessantes para nós, hackers, explorarmos

# PLACA GRÁFICA

A placa gráfica, ou, placa de vídeo, é um componente dedicado ao processamento de imagem.

Podemos considerar a placa gráfica como um segundo processador, porém com foco em paralelismo, ou seja, realiza diversas pequenas tarefas simultaneamente, com isso tendo um ótimo desempenho para processamento específico de imagens.

# COMO FUNCIONA UM SOFTWARE

Softwares são programas de computador.

Estes programas são escritos através de linguagens de programação, as quais, muitas vezes, se assemelham com a linguagem humana.

Todavia o computador não é capaz de interpretar a linguagem humana, e muito menos a própria linguagem de programação convencional utilizada pelos desenvolvedores

# COMO FUNCIONA UM SOFTWARE

O que acontece é um processo chamado de compilação e linkedição. Basicamente um outro software pega o conteúdo escrito pelo programador e traduz para código binário e em seguida vincula às funcionalidades escritas pelo programador às bibliotecas internas do sistema operacional.

# COMO FUNCIONA UM SOFTWARE

Linguagem de máquina ou linguagem binária é a linguagem escrita somente com números 0s e 1s.

Exemplo:

01100110 01111010 10010110  
10101111 11111101 11101011

# COMO FUNCIONA UM SOFTWARE

Todavia ler estes códigos seria extremamente complicado para o ser humano, e então análises mais aprofundadas do código de máquina seriam um verdadeiro inferno para os engenheiros.

Por conta disso foi desenvolvido uma "linguagem especial" chamada de ....



# COMO FUNCIONA UM SOFTWARE

Assembly, também sendo chamada de ASM como forma abreviada.

Esta linguagem na realidade não passa de mnemônico para os códigos binários.

Exemplo:

"10011111" se tornaria "ADD A"

O que é mais legível para os humanos, porém continuando com uma grande complexidade para programadores normais

# POR QUE ASSEMBLY?

Assembly, também sendo chamada de ASM como forma abreviada.

Esta linguagem na realidade não passa de mnemônico para os códigos binários.

Exemplo:

"10011111" se tornaria "ADD A"

O que é mais legível para os humanos, porém continuando com uma grande complexidade para programadores normais

# SUA PRIMEIRA ANÁLISE HACKING



Finalmente chegou a hora de por a mão na massa e fazer a sua primeira, análise.

Vou te guiar para que você entenda o funcionamento de uma análise básica em sites.

A partir disso você terá uma base para e aventurar por aí 😊

# Requisitos

Você vai precisar de:

- Navegador Google Chrome
- Paciência
- Persistência
- Vontade

Tudo certo?

Bora! 🚀



# Achando um Alvo

Escolha um site qualquer, que você já tenha algum certo conhecimento de como funciona (na visão de um usuário, não é necessário nenhum conhecimento interno do sistema em sí)

Como este é um e-book didático não vou referenciar nenhum site, mas farei um passo a passo com você

# Ativando a Ferramenta de Depuração

- Entre no site que você escolhe, através do google chrome
- Clique direito em qualquer área do site e escolha a opção "inspecionar", ou, "inspecionar elemento".

Exibir código fonte da página

Ctrl+U

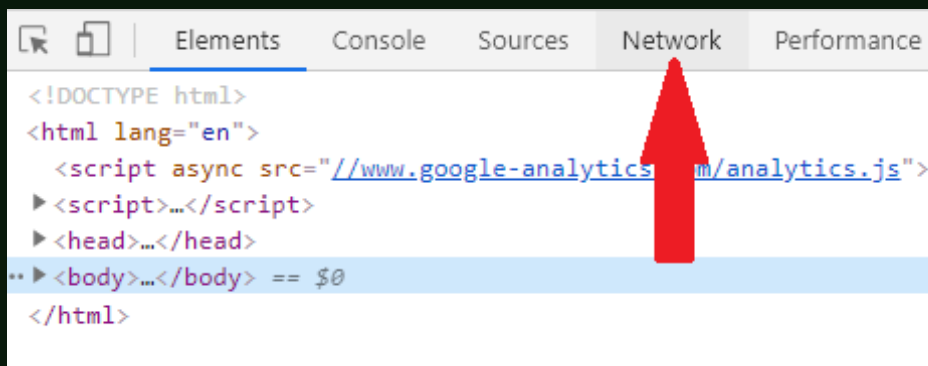
Inspeccionar

Ctrl+Shift+I



# Ativando a Ferramenta de Depuração

A ferramenta de desenvolvedor será aberta, e conterá diversos recursos. Nós iremos estudar a aba "network".



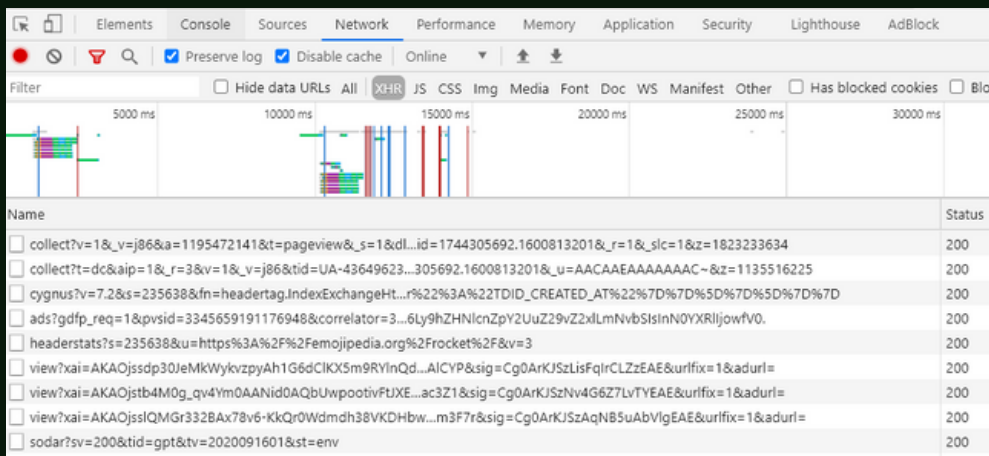
Este é um universo muito grande, de ferramentas, o qual abordo completamente no meu treinamento

**Guia Hacker**

# Depurando

Com a ferramenta aberta, atualize o site em que você está pressionando a tecla **F5**, do seu teclado

Você verá várias linhas aparecendo na ferramenta





# Entendendo

Estas linhas dizem respeito a todas as requisições que o site está fazendo para o sistema interno.

É por ai que os sites realizam alterações na tela do navegador, validam sua conexão com usuário e senha e muito mais.

Praticamente tudo que você faz pelo site passa por esta ferramenta

# Nosso Objetivo

Nosso Objetivo agora é analisar as requisições do tipo XHR, estas requisições são as mais utilizadas para passar dados de atualização, provindas do usuário.

Exemplo: Usuário digita login, senha e em seguida pressiona o botão "logar", ao pressionar o botão uma requisição XHR é feita passando as informações digitadas pelo usuário para o sistema interno do site.

Através da ferramenta network nós podemos visualizar esta requisição, e entender o que realmente está acontecendo.

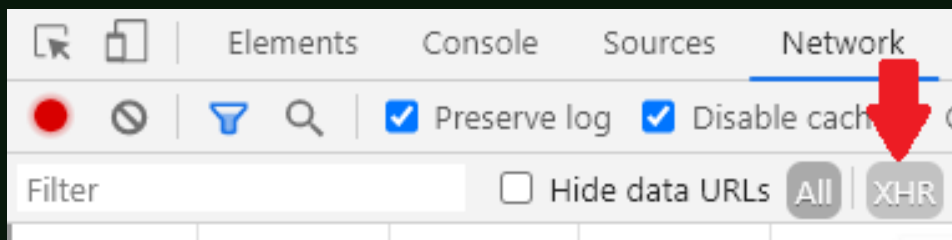
# Nosso Objetivo

Todavia, como não estamos trabalhando com um sistema definido, cada site terá seu próprio tipo de requisição. Então vou te ensinar de forma geral como analisar uma requisição

# Filtrando XHR

Vamos habilitar para que a ferramenta só mostre requisições do tipo XHR.

Basta escolher a opção XHR na ferramenta, como mostrado abaixo.



Em seguida atualize novamente a tela. Agora só deverá aparecer requisições do tipo XHR.

Lembrando que se você interagir com o site provavelmente novas requisições acontecerão para que você possa analisar.

# Analizando uma Requisição XHR

Escolha uma das linhas que foram geradas pela ferramenta.

*(Lembrando, o site que você está analisando pode ter linhas e conteúdos diferentes do meu exemplo)*

Name

☐ collect?v=1&\_v=j86&a=1195472141&t=pageview&s=1&dl...id=1744305692.1600813201&r=1&slc=1&z=1823233634

☐ collect?t=dc&aiP=1&r=3&v=1&\_v=j86&tid=UA-43649623...305692.1600813201&\_u=AACAEEAAAAAAC~&z=1135516225  
[https://www.google-analytics.com/jcollect?v=1&\\_v=j86&a=1195472141&t=pageview&s=1&dl=https%3A%2F%2Ffemojipedia.org%3Bcygnus%2F%2Fs%2F235638&n=headertag.indexExchangeHit%22%3A%22TDID\\_CREATED\\_AT%22%7D%7D%5D%7D%5D%7D%7D](https://www.google-analytics.com/jcollect?v=1&_v=j86&a=1195472141&t=pageview&s=1&dl=https%3A%2F%2Ffemojipedia.org%3Bcygnus%2F%2Fs%2F235638&n=headertag.indexExchangeHit%22%3A%22TDID_CREATED_AT%22%7D%7D%5D%7D%5D%7D%7D)

☐ ads?gdfp\_req=1&pvsid=3345659191176948&correlator=3...6Ly9hZHNlcnZpY2UzZnV2Z2xLmNvbSIsinN0YXRlbGwvO.

☐ headerstats?s=235638&u=https%3A%2F%2Ffemojipedia.org%2Frocket%2F&v=3

☐ view?xai=AKAOjsdp30JEkMkwyzvAhI6dClKX5m9RYInQd...AlCYP&sig=Cg0ArKJszLisFqrlCLZzEAE&urlfix=1&adurl=

☐ view?xai=AKAOjsbt4M0g\_qv4YmoDAANidQAQWUpwootivfJXE...ac3Z1&sig=Cg0ArKJszNv4G6Z7LvTYEAE&urlfix=1&adurl=

☐ view?xai=AKAOjsQMGr332BAx78v6-KKQr0wbhd38VFkdHbw...m3F7r&sig=Cg0ArKJszAQNB5AbVlgEAE&urlfix=1&adurl=

☐ sodar?sv=200&tid=gpt&tv=2020091601&st=env

☐ lgc

Basta escolher uma e clicar em cima,  
uma nova janela aparecerá na  
ferramenta

# Analizando uma Requisição XHR

Escolha uma das linhas que foram geradas pela ferramenta.

*(Lembrando, o site que você está analisando pode ter linhas e conteúdos diferentes do meu exemplo)*

Name

☐ collect?v=1&\_v=j86&a=1195472141&t=pageview&s=1&dl...id=1744305692.1600813201&r=1&slc=1&z=182323634

☐ collect?&dc&aip=1&\_r=3&v=1&\_v=j86&tid=UA-43649623...305692.1600813201&\_u=AACAAEAAAAAAAAA~&z=1135516225  
[https://www.google-analytics.com/jcollect?v=1&\\_v=j86&a=1195472141&t=pageview&s=1&dl=https%3A%2F%2Ffemojipedia.org%3Ccygnus?v=7&ds=235638&fn=headertag.IndexExchangeHit...r%22%3A%22TDID\\_CREATED\\_AT%22%7D%7D%5D%7D%5D%7D%7D](https://www.google-analytics.com/jcollect?v=1&_v=j86&a=1195472141&t=pageview&s=1&dl=https%3A%2F%2Ffemojipedia.org%3Ccygnus?v=7&ds=235638&fn=headertag.IndexExchangeHit...r%22%3A%22TDID_CREATED_AT%22%7D%7D%5D%7D%5D%7D%7D)

☐ ads?gdfp\_req=1&pvsid=3345659191176948&correlator=3...6Ly9hZHlnClncZpY2UzZ9V2ZlXmNvbSisinN0YXRljowfv0.

☐ headerstats?v=235638&u=https%3A%2F%2Ffemojipedia.org%2Frocket%2F&v=3

☐ view?xai=AKAOjsdp30JemKWykvyqAh1G6dCLIX5m9RYInQd...ALCPY&sig=Cg0ArKJSzLisFqlrCLZzEAE&urlfix=1&adurl=

☐ view?xai=AKAOjstb4M0g\_qv4YmOANid0AQbUwpootivfJXE...ac3Z1&sig=Cg0ArKJSzNv4G6Z7LvTYEAE&urlfix=1&adurl=

☐ view?xai=AKAOjslQMGR32B8Ax7v86-KkQrOWdmhd38VKDHbw...m3F7r&sig=Cg0ArKJSzAqNB5uAbVlgEAE&urlfix=1&adurl=

☐ sodar?sv=200&tid=gpt&tv=2020091601&st=env

☐ lgc

Basta escolher uma e clicar em cima,  
uma nova janela aparecerá na  
ferramenta

# **Analisando uma Requisição XHR**

Está nova Janela conterá outras sub-abas. Nós iremos analisar a "Headers" e a "Preview".

No headers veremos os valores que foram enviados

No preview veremos os valores que vieram como resposta do servidor

# Analizando o Header

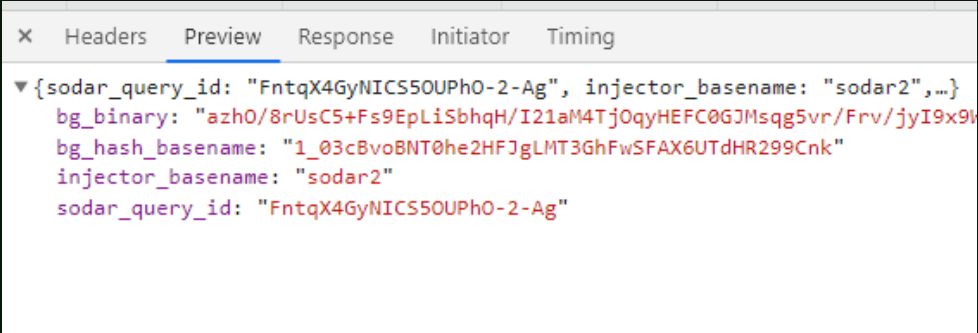
No Header iremos rolar para baixo até encontramos a área "Query String Parameters", ali terá o conteúdo que saiu do nosso navegador para o servidor

▼ Query String Parameters	<a href="#">view source</a>	<a href="#">view decoded</a>
<b>t:</b> dc		
<b>aip:</b> 1		
<b>_r:</b> 3		
<b>v:</b> 1		
<b>_v:</b> j86		
<b>tid:</b> UA-43649623-1		
<b>cid:</b> 1829655685.1595460209		
<b>jid:</b> 1484389833		
<b>gjid:</b> 997060804		
<b>_gid:</b> 1744305692.1600813201		
<b>_u:</b> AACAAEAAAAAAC~		
<b>z:</b> 1135516225		



# Analizando o Preview

O Preview é uma apresentação processada do resultado da aba "response". Aqui nós podemos ver o que foi respondido pelo servidor com relação a requisição que foi feita e de acordo com os parâmetros enviados

A screenshot of a network analysis tool's interface, specifically the 'Preview' tab. The tab is selected and underlined. Above it are other tabs: 'Headers', 'Response', 'Initiator', and 'Timing'. The main area displays a JSON object with several fields. The first field is 'sodar\_query\_id' with a long alphanumeric string. The second is 'injector\_basename' with the value 'sodar2'. The third is 'bg\_binary' with a long alphanumeric string. The fourth is 'bg\_hash\_basename' with a long alphanumeric string. The fifth is 'injector\_basename' with the value 'sodar2'. The sixth is 'sodar\_query\_id' with the same long alphanumeric string as the first field. The JSON is formatted with red text for the keys and black text for the values.

```
▼ {sodar_query_id: "FntqX4GyNICS50UPhO-2-Ag", injector_basename: "sodar2", ...}
  bg_binary: "azhO/8rUsC5+F59EpLiSbhqH/I21aM4TjOqyHEFC0GJM5qg5vr/Frv/jyI9x9v
  bg_hash_basename: "1_03cBvoBNT0he2HFJgLMT3GhFwSFAX6UTdHR299Cnk"
  injector_basename: "sodar2"
  sodar_query_id: "FntqX4GyNICS50UPhO-2-Ag"
```

# **O que posso fazer com tudo isso?**

Simples. Agora você tem acesso ao que vai e volta do servidor; chegou a hora de analisar os dados trafegados e entender o que fazem.

Com isso você poderá encontrar diversas falhas em vários sistemas ao redor da internet

# O que você aprendeu?

Até agora você aprendeu diversos conceitos extremamente importantes sobre computação e hacking.

Entendeu como funcionam os componentes internos do computador, como um site funciona através de requisições do tipo XHR

E aprendeu até mesmo a analisar facilmente um sistema web.

Porém...

# O PRÓXIMO PASSO

A partir daqui você tem dois caminhos...

O primeiro é trilhar sozinho em busca de mais informações e descobrir por conta própria como fazer estas análises de forma eficaz.

E eu vou ser sincero. Isso vai ser muito difícil, pois não há nada sobre isso aberto pela internet.

A outra opção é...

# O PRÓXIMO PASSO

Adentrar para o meu club de alunos em hacking.

Estou te convidando para conhecer o meu treinamento especializado em segurança da informação. Analise de falhas e quebra de sistemas.

O Guia Hacker é um treinamento voltado para levar o iniciante do absoluto zero até o hacking, recebendo certificações e tornando-se um verdadeiro profissional da área...

# O PRÓXIMO PASSO

Caso você tenha interesse em revolucionar completamente a sua vida...

Podendo ingressar em um mercado pouco explorado e muito lucrativo.

E ainda trabalhar para grandes corporações ao redor do mundo, sem precisar sair da sua casa de forma remota, através da internet.

Tudo isso e muito mais.





Conheça meu treinamento clicando aqui: <https://guiahacker.com>

# PEDIDO!

Preste ATENÇÃO...

Obrigado por ter lido até aqui  
Espero que possamos nos encontrar  
em breve em outros conteúdos  
sobre hacking.

Mas antes de partir, quero te pedir  
uma coisa.

Envie-me um e-mail dizendo o que  
achou sobre o e-book. Isso seria  
muito legal e eu ficaria bem feliz  
( ° ° )   ( ° °  )

Manda lá: [contato@guiahacker.com](mailto:contato@guiahacker.com)