3 PASSOS PARA APPS MAIS SEGUROS

Agenda

- Jogue no **Red Team**
- Melhore remotamente
- Informe-se

Jogue no Red Team

Jogue no Red Team

- Intercepte tráfego com Charles ou BurpSuite
- Faça **jailbreak**, info em /r/jailbreak
- Consiga os dados do seu bundle
- Use **Clutch** para descriptografar o executável do app
- Analise seu binário com **Hopper**
- Injete código em runtime com **Cycript**

Jogue no Red Team

- Intercepte tráfego com Charles ou BurpSuite
- Faça **jailbreak**, info em /r/jailbreak
- Consiga os dados do seu bundle
- Use **Clutch** para descriptografar o executável do app
- Analise seu binário com **Hopper**
- Injete código em runtime com **Cycript**

Jogue no Red Team

- Intercepte tráfego com Charles ou BurpSuite
- Faça **jailbreak**, info em /r/jailbreak
- Consiga os dados do seu bundle
- Use **Clutch** para descriptografar o executável do app
- Analise seu binário com **Hopper**
- Injete código em runtime com **Cycript**

Jogue no Red Team

- Intercepte tráfego com Charles ou BurpSuite
- Faça **jailbreak**, info em /r/jailbreak
- Consiga os dados do seu bundle
- Use **Clutch** para descriptografar o executável do app
- Analise seu binário com **Hopper**
- Injete código em runtime com **Cycript**

Jogue no Red Team

- Intercepte tráfego com Charles ou BurpSuite
- Faça **jailbreak**, info em /r/jailbreak
- Consiga os dados do seu bundle
- Use **Clutch** para descriptografar o executável do app
- Analise seu binário com **Hopper**
- Injete código em runtime com **Cycript**

Jogue no Red Team

- Intercepte tráfego com Charles ou BurpSuite
- Faça **jailbreak**, info em /r/jailbreak
- Consiga os dados do seu bundle
- Use **Clutch** para descriptografar o executável do app
- Analise seu binário com **Hopper**
- Injete código em runtime com **Cycript**

Melhore remotamente

Melhore remotamente

- Não confie na **API**
- Remover **allow arbitrary loads**
- Use **SSL Pinning**
- Converse com os outros times

Melhore remotamente

- Não confie na **API**
- Remover **allow arbitrary loads**
- Use **SSL Pinning**
- Converse com os outros times

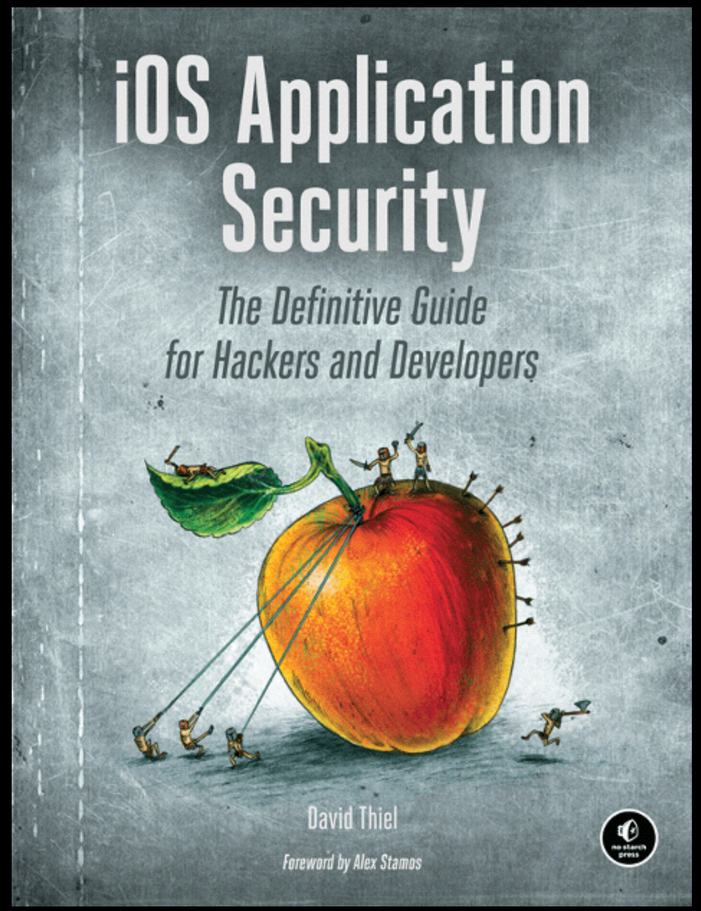
Melhore remotamente

- Não confie na **API**
- Remover **allow arbitrary loads**
- Use **SSL Pinning**
- Converse com os outros times

Melhore remotamente

- Não confie na **API**
- Remover **allow arbitrary loads**
- Use **SSL Pinning**
- Converse com os outros times

Informe-se



- black hat
- def con
- derby con
- bsides

@thehackbr
@mikko
@SwiftOnSecurity

/r/netsec
/r/hackernews
/r/jailbreak

Perguntas?

whoami

@kuquert

guidebook