Web Application Security

Михаил Щербаков

Обо мне

- IT безопасность: статический и динамический анализ кода, безопасность web-приложений
- IT конференции: спикер, соорганизатор .NET митапов в Санкт-Петербурге и Москве, член программного комитета DotNext
- Microsoft .NET Most Valuable Professional (MVP)
- Удаленная работа: Top Rated фрилансер на Upwork, больше года в свободном плаванье
- Учился/работал: ПГТА, Парус-Пенза, НПФ КРУГ, Luxoft, Boeing, Acronis, Positive Technologies, Cezurity
- Хобби: бег, виндсерфинг, самостоятельные путешествия

О чем пойдет речь?

- Системный подход к разработке защищенных web-приложений

О чем пойдет речь?

- ~~Системный подход к разработке защищенных web-приложений~~

  https://www.youtube.com/watch?v=mb7tcT-9VXk

  https://www.youtube.com/watch?v=hKatpz72EpE

О чем пойдет речь?

- ~~Системный подход к разработке защищенных web-приложений~~

  https://www.youtube.com/watch?v=mb7tcT-9VXk

  https://www.youtube.com/watch?v=hKatpz72EpE

- Мифы/ошибки/недопонимание возможностей проведения атак на web-приложения

О чем пойдет речь?

- ~~Системный подход к разработке защищенных web-приложений~~

  https://www.youtube.com/watch?v=mb7tcT-9VXk

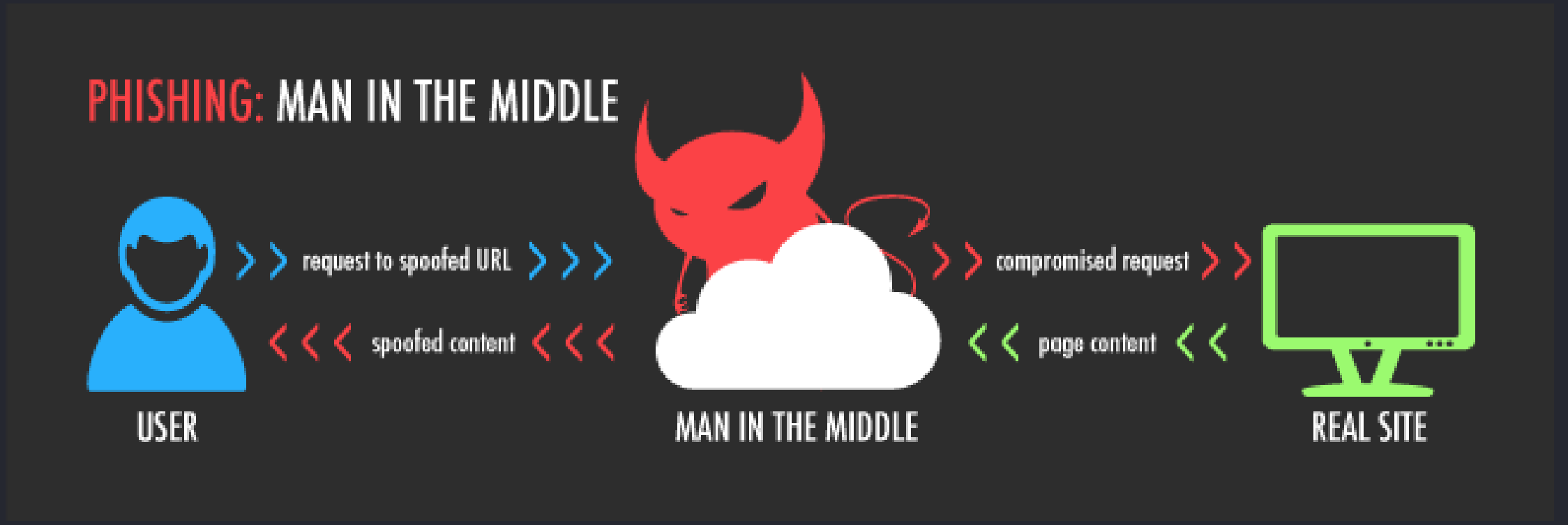
  https://www.youtube.com/watch?v=hKatpz72EpE
- Мифы/ошибки/недопонимание возможностей проведения атак на web-приложения
- Все примеры под .NET, а почему бы и нет

Миф №1: Я использую HTTPS, значит мой сайт защищен

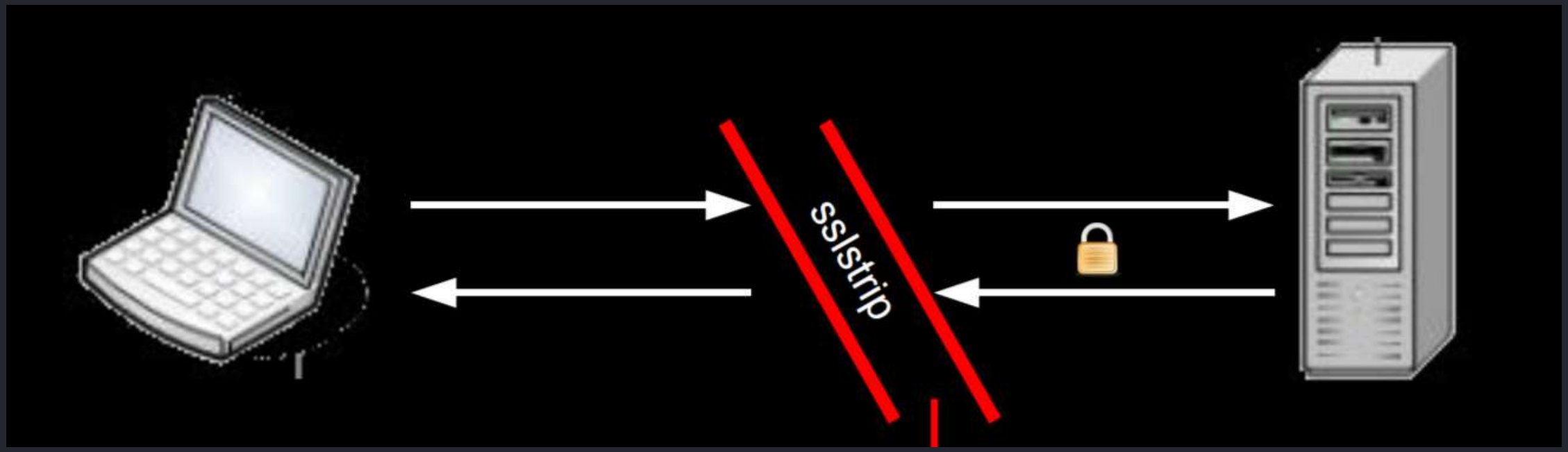
Миф №1: ~~Я использую HTTPS, значит мой сайт защищен~~

Миф №1: HTTPS всегда защищает от Man-in-the-Middle атак

Man-in-the-Middle (MitM)

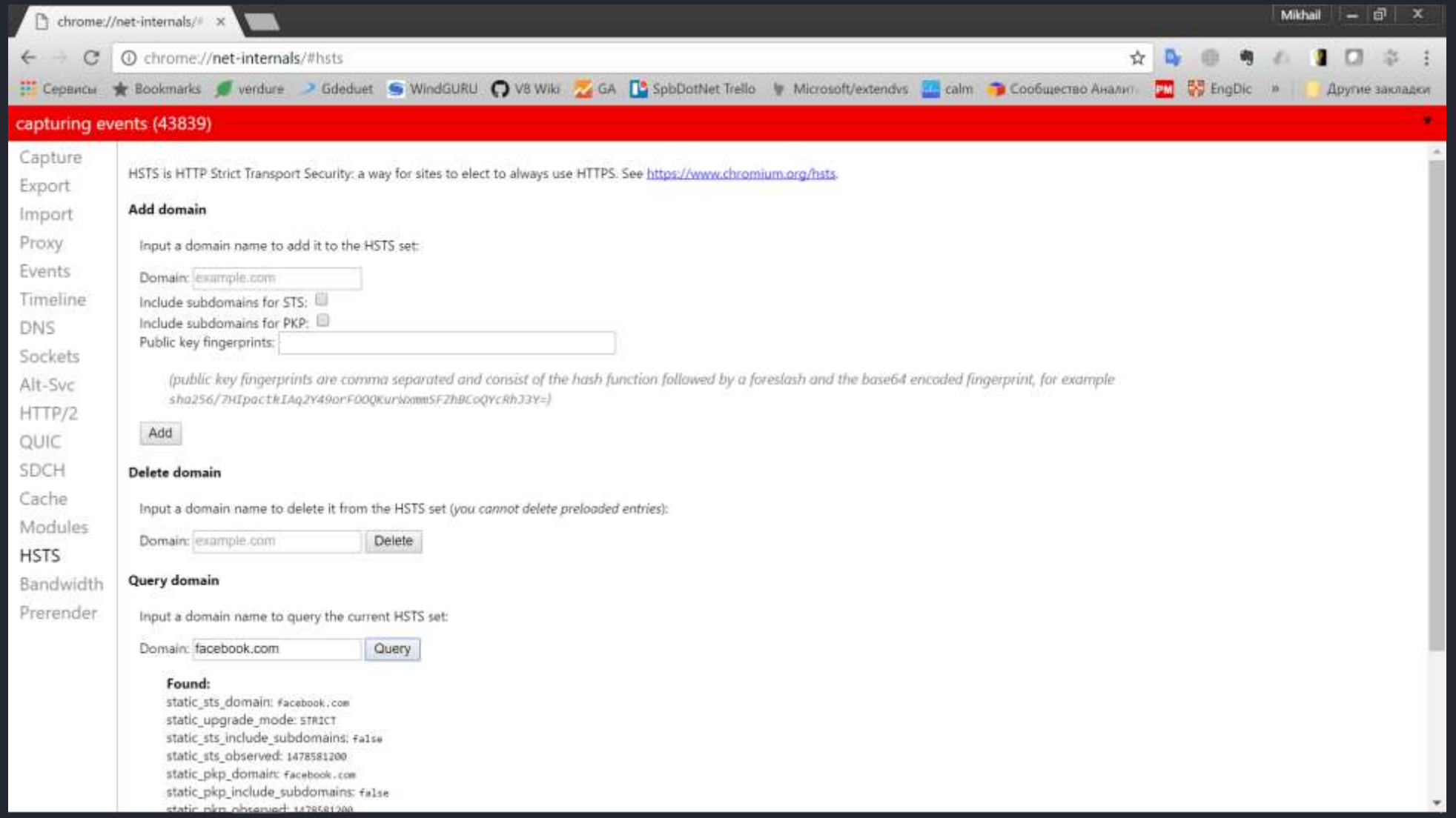


SSL Stripping



https://www.youtube.com/watch?v=MFol6IMbZ7Y

HTTP Strict Transport Security



Обход HSTS

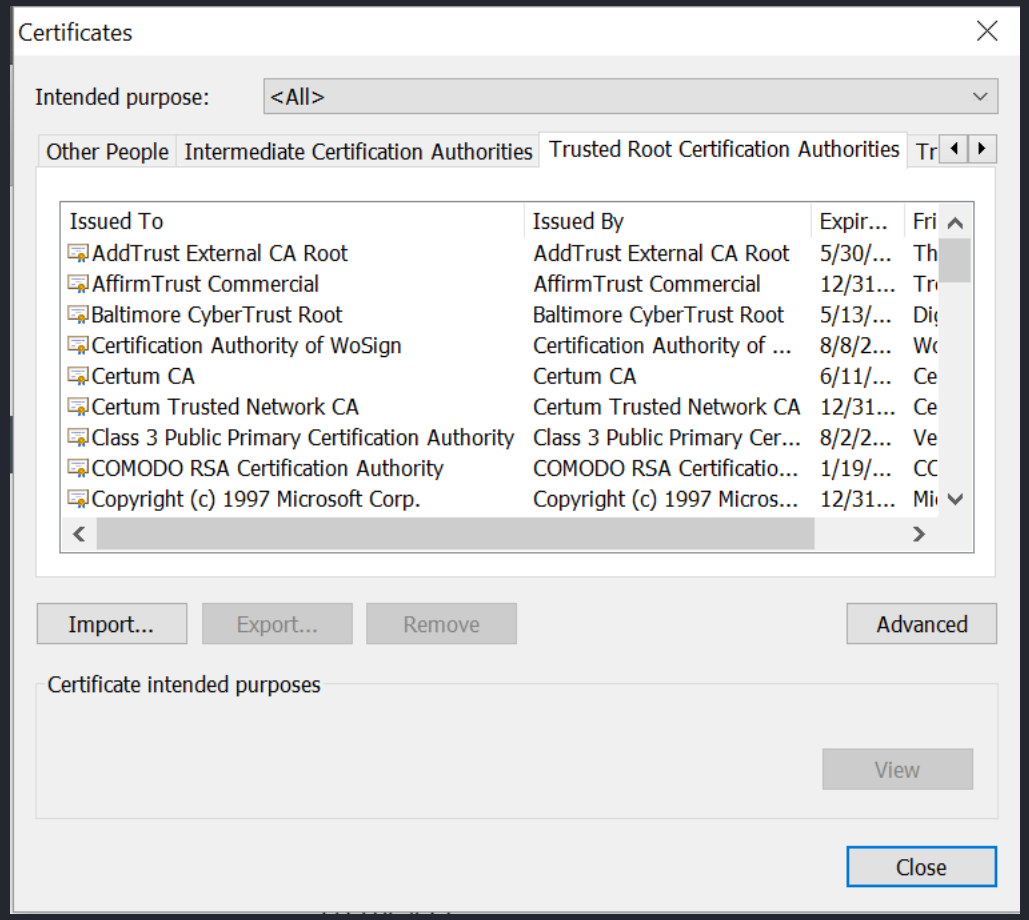
- Black Hat Europe 2014 - Jose Selvi “BYPASSING HTTP STRICT TRANSPORT SECURITY”

https://www.blackhat.com/eu-14/briefings.html#bypassing-http-strict-transport-security

- Black Hat Asia 2014 - Leonardo Nve “OFFENSIVE: EXPLOITING DNS SERVERS CHANGES”

https://www.blackhat.com/docs/asia-14/materials/Nve/Asia-14-Nve-Offensive-Exploiting-DNS-Servers-Changes.pdf

Доверенные корневые сертификаты. Ты им всем доверяешь?



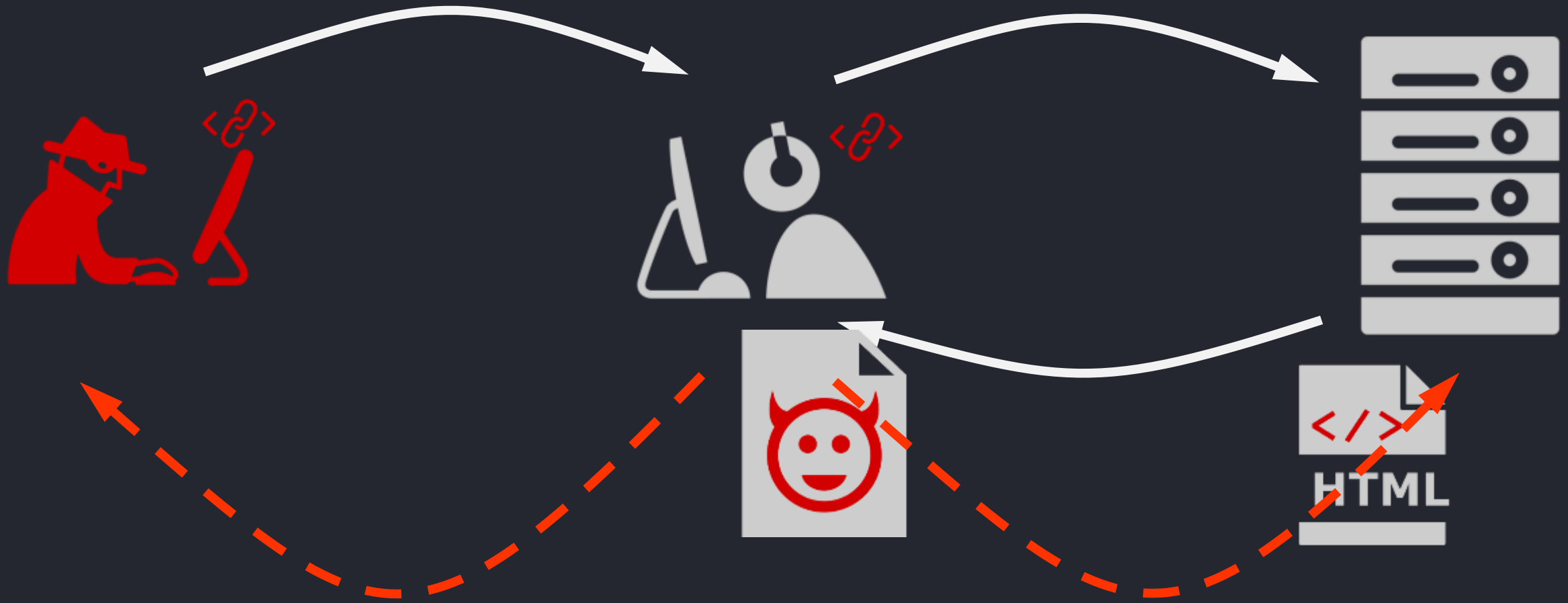
Центры сертификации

- Нарушения стандартов WoSign и StartCom
- Атаки на COMODO, DIGINOTAR, GLOBALSING
- И другие инциденты https://git.cryto.net/joepie91/ca-incidents

HTTPS защищает *опытных* пользователей от *массового* перехвата трафика *часто используемого* web-ресурса

Миф №2: Последняя версия JQuery не уязвима к XSS атакам

Reflected XSS

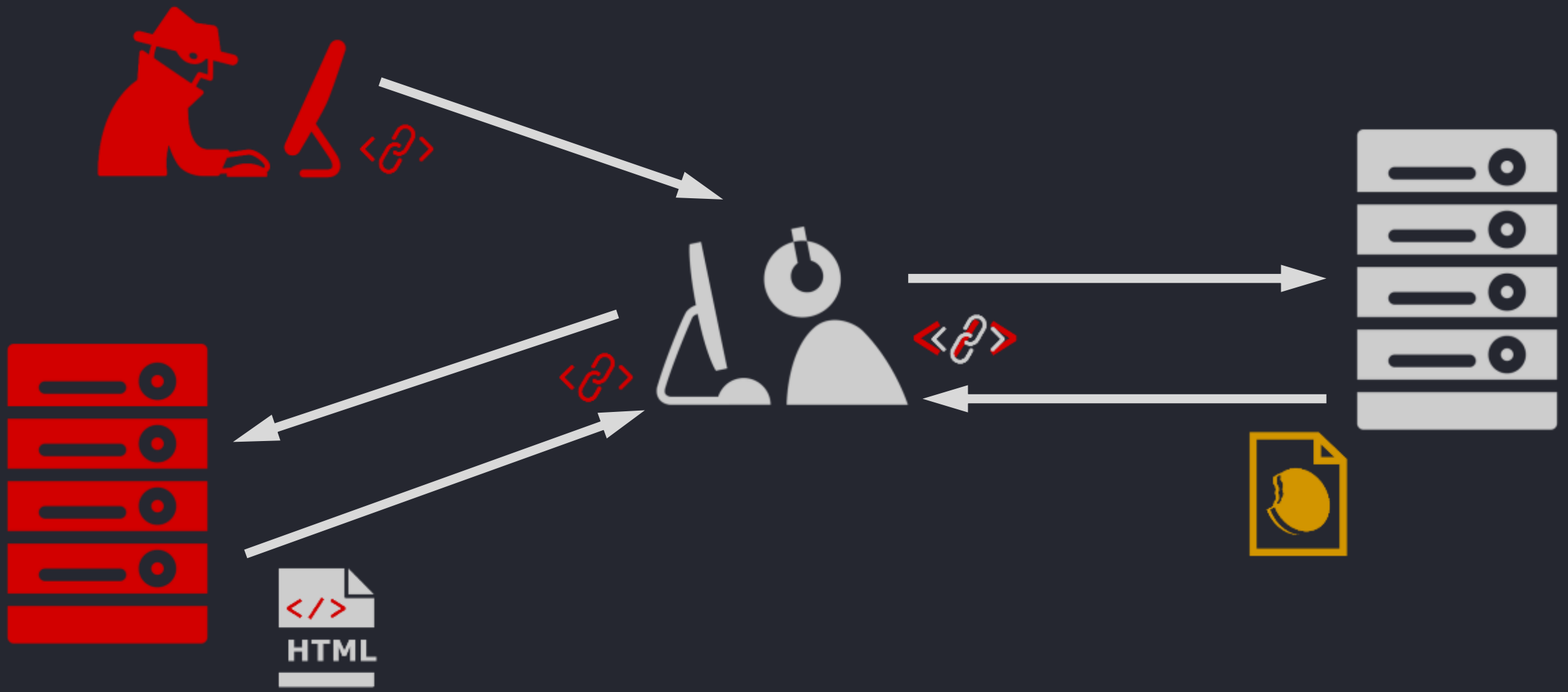


JQuery Demo

Миф №3: XSS на мало посещаемом ресурсе неопасна!

- Да сюда пользователи не ходят
- Этот сайт не работает с конфиденциальными данными
- Все наши cookies с HttpOnly

CSRF via XSS



Session Fixation Demo

Миф №4: Нельзя проэксплуатировать XMLi/XXE, если я не возвращаю ничего пользователю

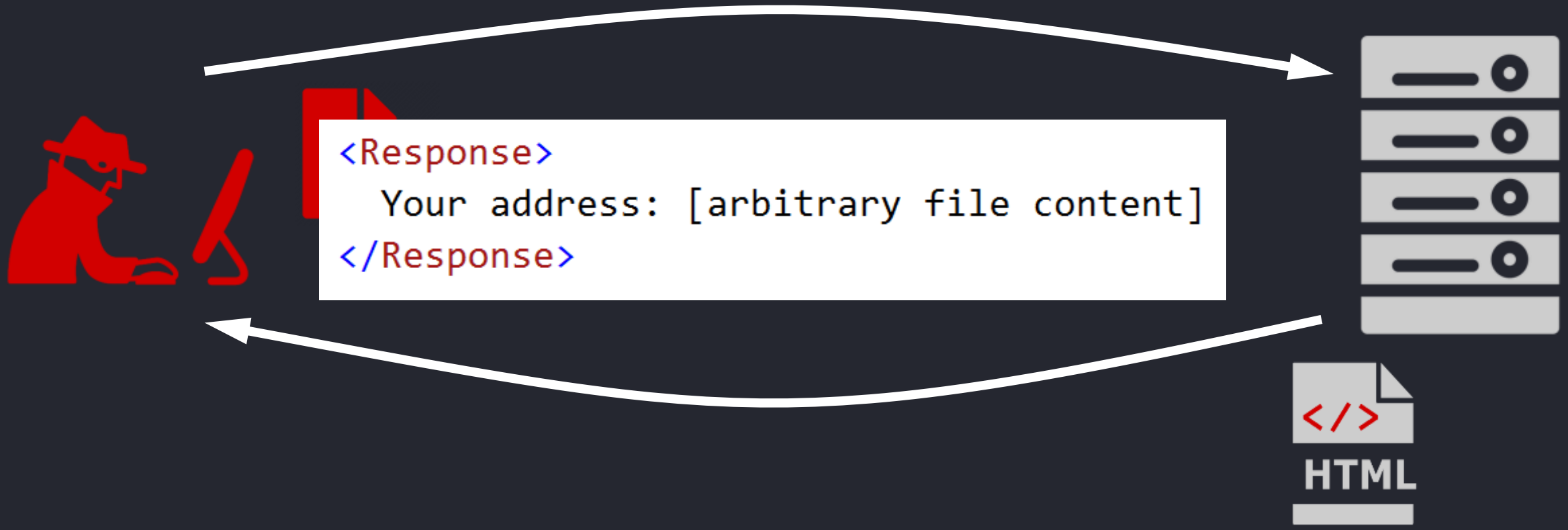
XML Entity

```
1   <?xml version="1.0" encoding="utf-8" ?>
2   <!DOCTYPE catalog [
3     <!ENTITY msg "Hello Word">
4   ]>
5   <catalog>
6     <person>
7       <gAddress>&msg;</gAddress>
8       <gAge>18</gAge>
9       <gPhone>777-777-777</gPhone>
10    </person>
11  </catalog>
```

XML External Entity

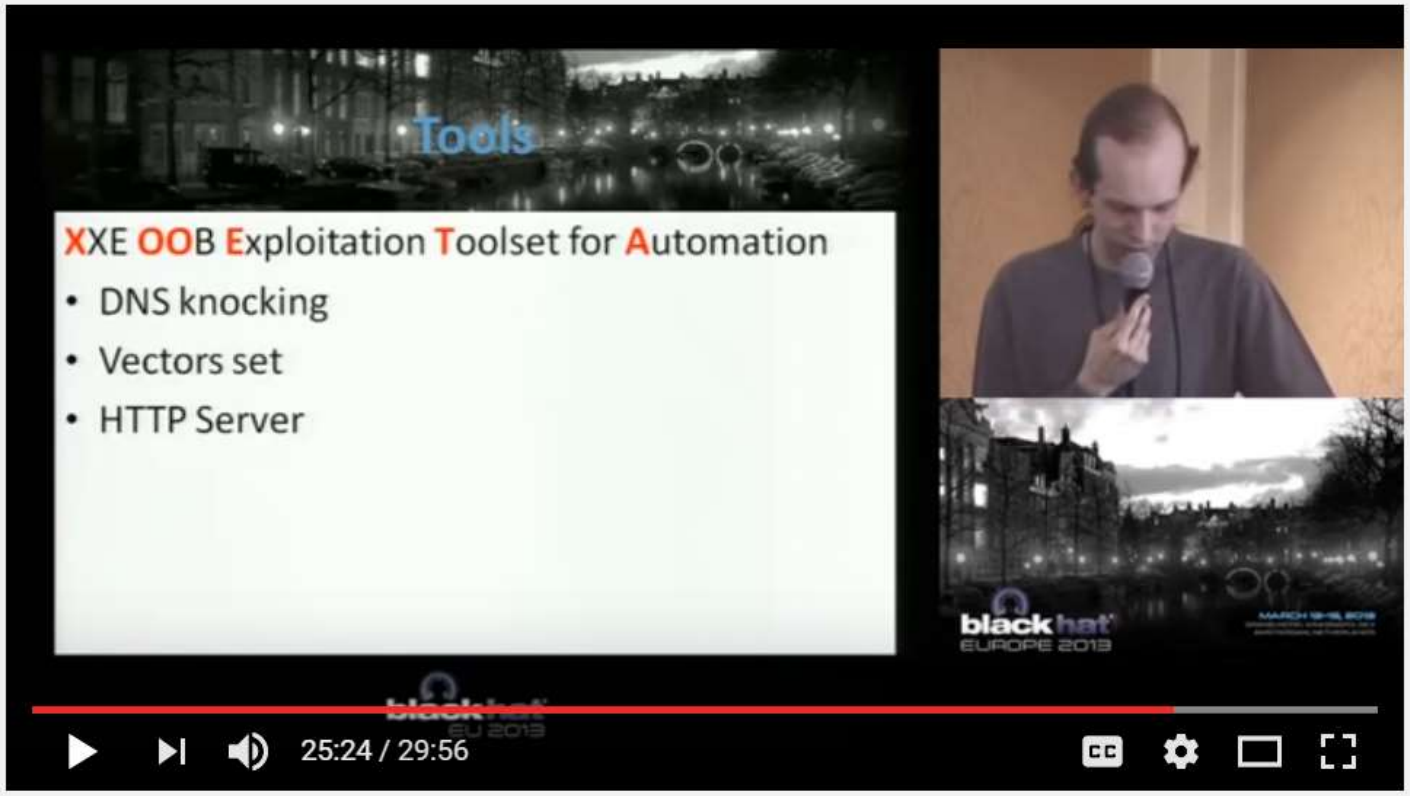
```
1   <?xml version="1.0" encoding="utf-8" ?>
2   <!DOCTYPE catalog [
3     <!ENTITY msg SYSTEM "file:///c:/inetpub/project/Web.config">
4   ]>
5   <catalog>
6     <person>
7       <gAddress>&msg;</gAddress>
8       <gAge>18</gAge>
9       <gPhone>777-777-777</gPhone>
10    </person>
11  </catalog>
```

Classic XXE Attack



XXE Attack Demo

XML Out-of-Band Data



A.Osipov, T.Yunusov 2013
“XML OOB Data Retrival”
https://youtu.be/eBm0YhBrT_c

T.Morgan 2014
“XML Schema, DTD, and Entity Attacks”
http://bit.ly/2h6wtTH

Billion Laughs Attack

```
1  <?xml version="1.0" encoding="utf-8" ?>
2  <!DOCTYPE catalog [
3    <!ENTITY a0 "dos" >
4    <!ENTITY a1 "&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;">
5    <!ENTITY a2 "&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;">
6    <!ENTITY a3 "&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;">
7    <!ENTITY a4 "&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;">
8  ]>
9  <catalog>
10   <person>
11     <gAddress>&a4;</gAddress>
12   </person>
13 </catalog>
```

Как исправить?

- Prohibit DTD processing
- Nullify references to resolvers
- Utilize a secure resolver
- Limit expansion size and set default timeouts

Итог

- OWASP Top Ten Project 2013 http://bit.ly/1OffewO
- SSL and TLS Deployment Best Practices http://bit.ly/2aSNEEg
- OWASP Developer Guide http://bit.ly/1JcQLoh
- OWASP .NET Security Cheat Sheet http://bit.ly/2h2fDrQ
- Tom FitzMacken “What not to do in ASP.NET, and what to do instead” http://bit.ly/2h2sfyU

Спасибо!

Михаил Щербаков

Независимый разработчик и консультант

linkedin.com/in/mikhailshcherbakov

spbdotnet.org

mskdotnet.org

@yu5k3