



MYTHBUSTERS

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 плавании
- **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

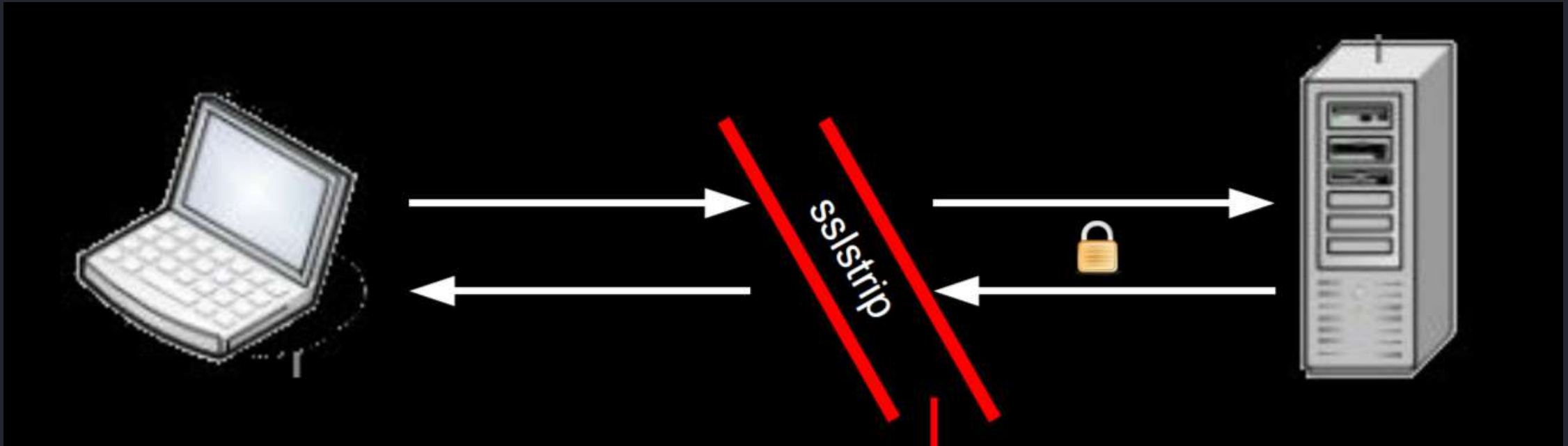
Миф №1: HTTPS всегда
защищает от
Man-in-the-Middle атак

Man-in-the-Middle (MitM)

PHISHING: MAN IN THE MIDDLE



SSL Stripping



<https://www.youtube.com/watch?v=MFo16IMbZ7Y>

HTTP Strict Transport Security

The screenshot shows the Chrome://net-internals/#hsts page in a browser window. The address bar shows 'chrome://net-internals/#hsts'. The page has a red header bar that says 'capturing events (43839)'. On the left is a sidebar with navigation links: Capture, Export, Import, Proxy, Events, Timeline, DNS, Sockets, Alt-Svc, HTTP/2, QUIC, SDCH, Cache, Modules, HSTS, Bandwidth, and Prerender. The main content area has a heading 'HSTS is HTTP Strict Transport Security: a way for sites to elect to always use HTTPS. See <https://www.chromium.org/hsts>.' Below this are three sections: 'Add domain', 'Delete domain', and 'Query domain'. The 'Add domain' section has a text input for 'Domain' with 'example.com' entered, and two checkboxes for 'Include subdomains for STS' and 'Include subdomains for PKP', both of which are unchecked. There is also a text input for 'Public key fingerprints'. Below these inputs is a paragraph of text explaining the format for public key fingerprints, followed by an 'Add' button. The 'Delete domain' section has a text input for 'Domain' with 'example.com' entered and a 'Delete' button. The 'Query domain' section has a text input for 'Domain' with 'facebook.com' entered and a 'Query' button. Below the 'Query' button, the results of the query are displayed under the heading 'Found:'. The results are as follows:

```
static_sts_domain: facebook.com
static_upgrade_mode: STRICT
static_sts_include_subdomains: false
static_sts_observed: 1478581200
static_pkp_domain: facebook.com
static_pkp_include_subdomains: false
static_pkp_observed: 1478581200
```

Обход HSTS

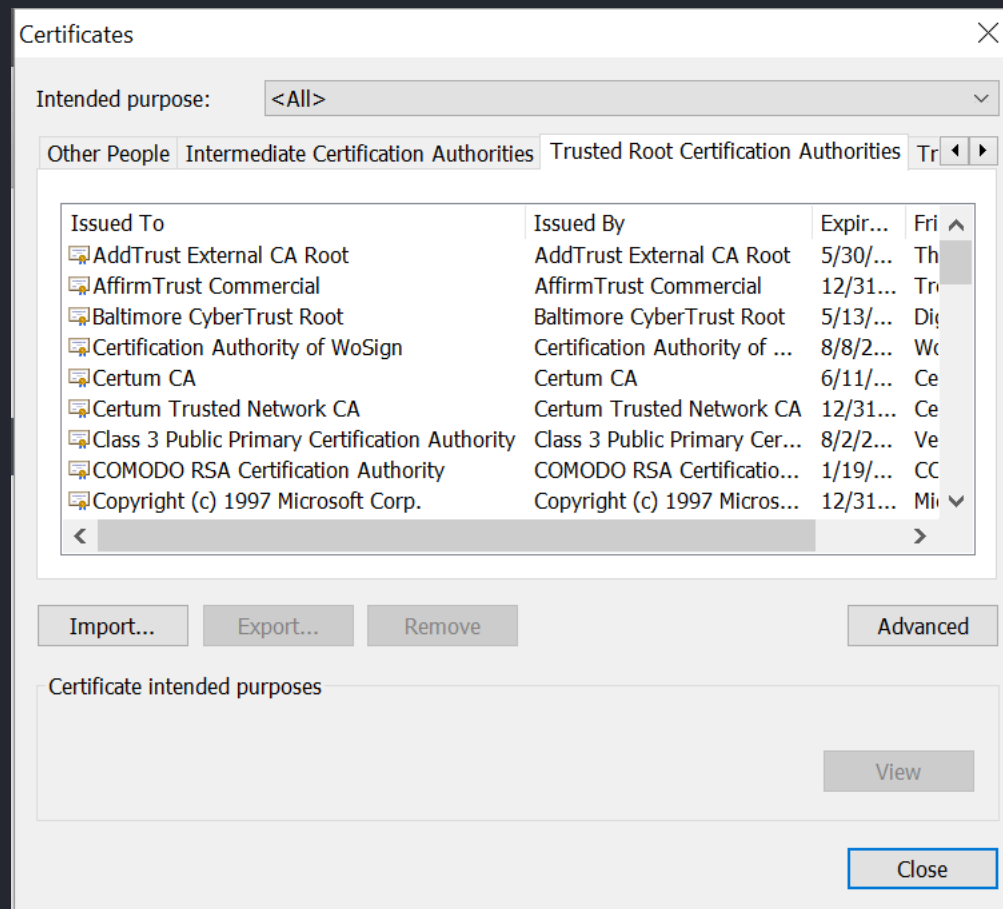
- Black Hat Europe 2014 - Jose Selvi “BYPASSING HTTP STRICT TRANSPORT SECURITY”

<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

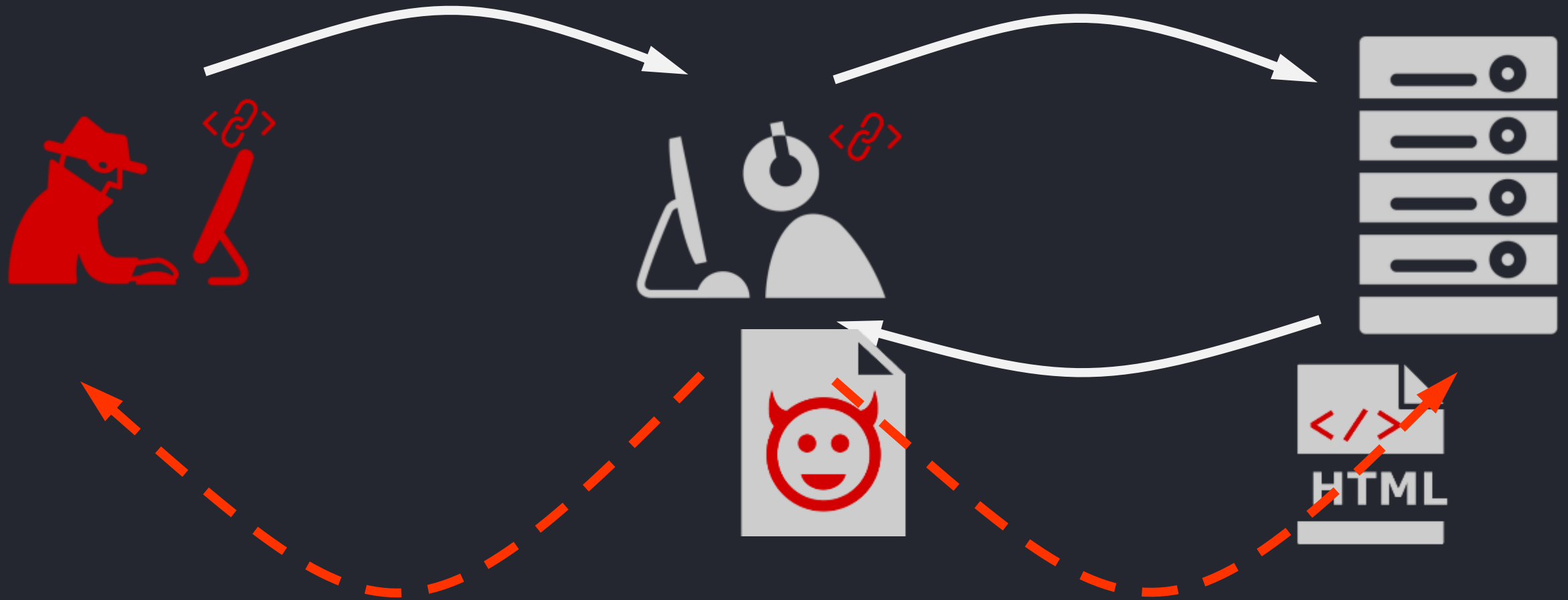
- Нарушения стандартов WoSign и StartCom
- Атаки на COMODO, DIGINOTAR, GLOBALSING
- И другие инциденты
<https://git.cryto.net/joepie91/ca-incidents>

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



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

Reflected XSS



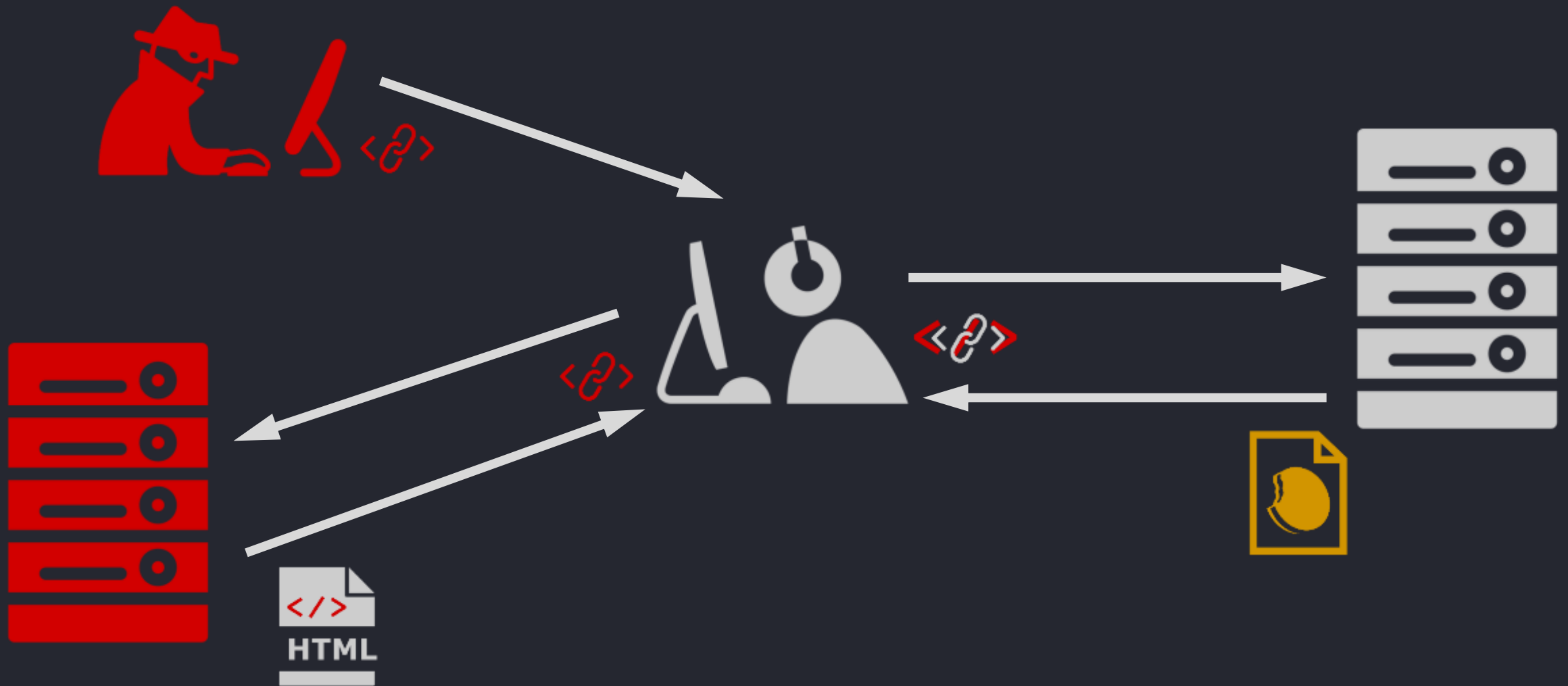
JQuery Demo



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

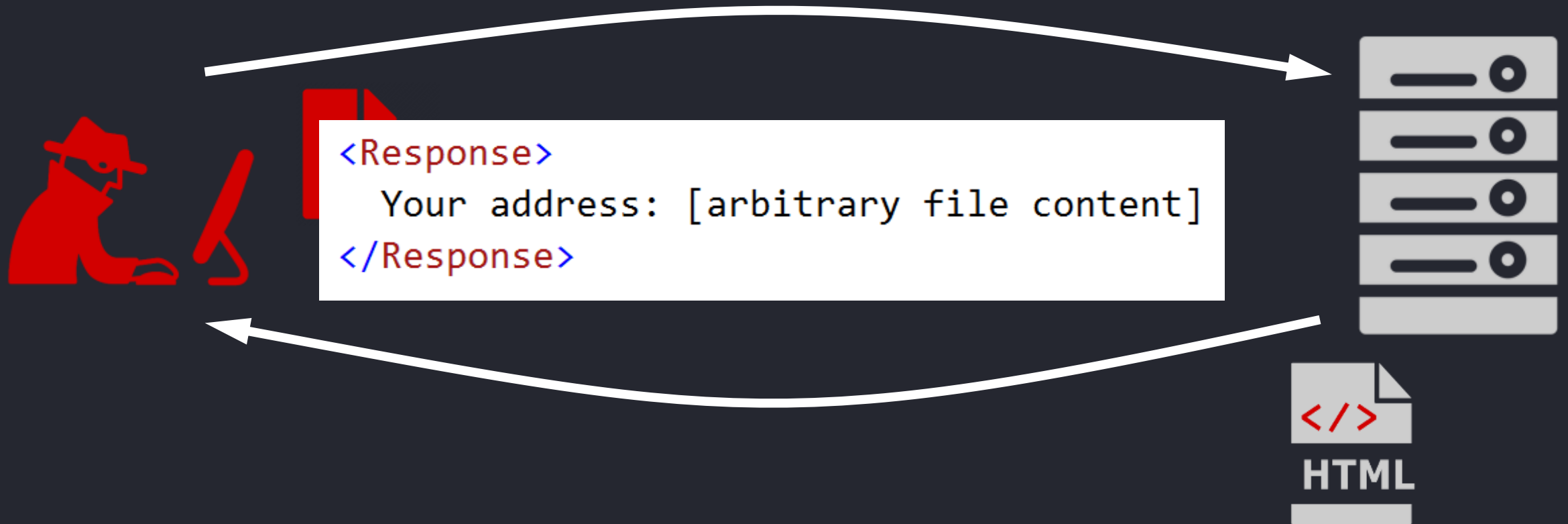
XML Entity

```
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>
```

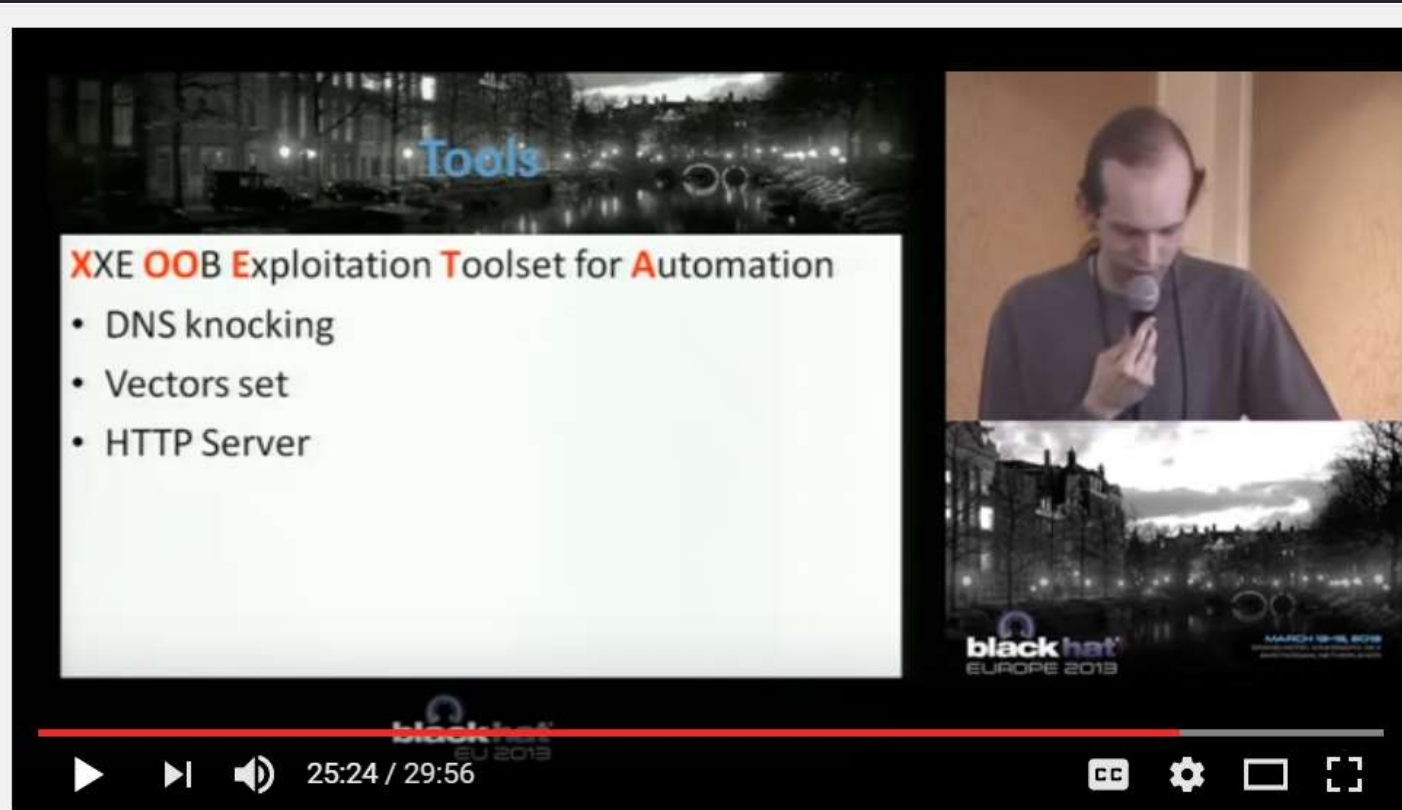
Classic XXE Attack



XXE Attack Demo



XML Out-of-Band Data



Black Hat EU 2013 - XML Out-of-Band Data Retrieval

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/10ffew0>
- 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