2000.00.00

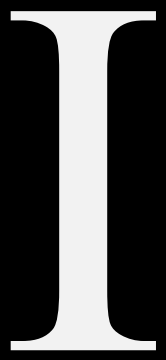
File upload & XXE

가디언 웹 보안 세미나 6

발표자

File Upload 1

Path traversal



Upload vulnerabilty

정의

파일업로드 과정의 취약점

name, type, contents, or size

이것들에 대한 validation이 없을 경우

파일 업로드 + 추가 payload로 실행

중심에서 0.3cm 떨어진 소속 18px

Upload vulnerabilty

이후…

→ XSS (stored XSS)

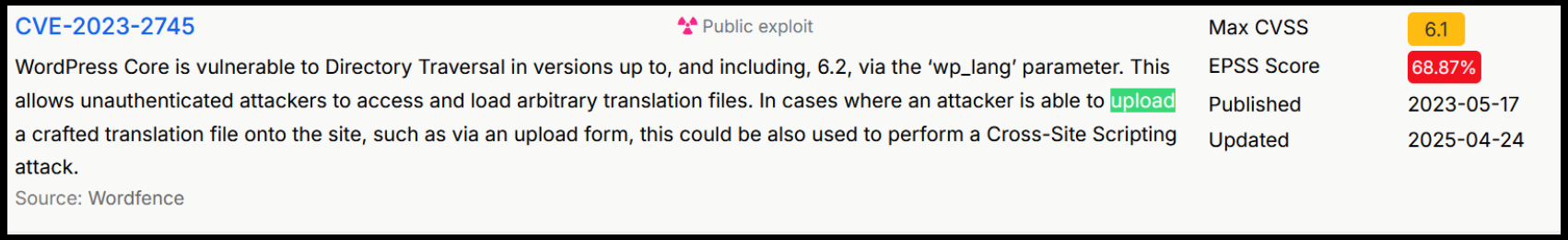
→ Webshell

서버를 통해 shell이 열린다.

중심에서 0.3cm 떨어진 소속 18px

Upload vulnerabilty

Example



Path Traversal → XSS

중심에서 0.3cm 떨어진 소속 18px

Path Traversal

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 2 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 3 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px

중심에서 0.3cm 떨어진 소속 18px

실습? [file-download-1]

http://dreamhack.io/wargame/challenges/37

매우 간단한 path-traversal !

중심에서 0.3cm 떨어진 소속 18px

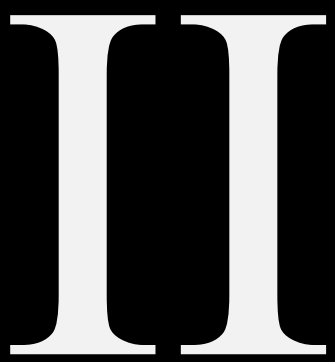
실습? [filestorage]

http://dreamhack.io/wargame/challenges/643

중심에서 0.3cm 떨어진 소속 18px

File Upload 2

Web shell



PHP?

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 2 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 3 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

1cm-1cm 떨어진 주석 12px

php webshell은 MS Defender에서 삭제시킨다.

중심에서 0.3cm 떨어진 소속 18px

Webservers

Default behavior이 다르다

Apache php 파일 기본 실행

mod_php 설치시 default

Nginx php 파일 기본 실행 x

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px

중심에서 0.3cm 떨어진 소속 18px

Webservers

Nginx

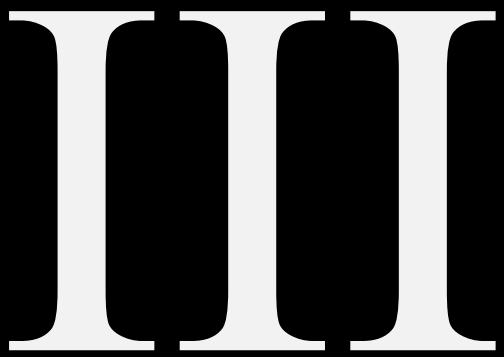
```
location ~ .php$ {
  include fastcgi_params;
  fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
  fastcgi_pass 127.0.0.1:9000;
}
```

Nginx wiki에서 흔한 실수들을 읽을 수 있다.

중심에서 0.3cm 떨어진 소속 18px

XXE

Vunerable XML



Extensible Markup Language

XML

데이터 구조를 정의하는 언어

구조화 / 확장성

https://www.w3.org/TR/xml/

중심에서 0.3cm 떨어진 소속 18px

Extensible Markup Language

XML

```xml
<note>
    <to>you</to>
    <from>me</from>
    <heading>Note</heading>
    <body>XML it is</body>
</note>
```

https://www.w3.org/TR/xml/

중심에서 0.3cm 떨어진 소속 18px

Extensible Markup Language

Basics

```
<!-- This is an element -->
<note>
    <element>value</element>
</note>
<!-- This is an attribute -->
<note attribute="value">
</note>
```

중심에서 0.3cm 떨어진 소속 18px

Extensible Markup Language

Namespace

```xml
<!-- Define a namespace -->
<!-- The syntax is xmlns:prefix="URI" -->
<note xmlns:example="http://www.example.com">
    <!-- Use the namespace -->
    <!-- The syntax is prefix:tagname -->
    <example:to>you</example:to>
    <example:from>me</example:from>
    <example:heading>Note</example:heading>
    <example:body>XML it is</example:body>
    <comment example:date="2025-0805">Attribute can be defined over namespace</comment>
</note>
```

겹치는 element나 attribute를 구분하게 해준다.

중심에서 0.3cm 떨어진 소속 18px

DTD

XML

XML 구조를 정의할 수 있는 문법

이름, 엔티티 등을 정의

내부 / 외부 DTD

Document Type Definition

중심에서 0.3cm 떨어진 소속 18px

DTD

XML

```xml
<!-- note.xml -->
<!DOCTYPE note SYSTEM "note.dtd">
...

<!-- note.dtd -->
<!ELEMENT note (to, from, heading, body)>
<!ELEMENT to (#PCDATA)>
<!ELEMENT from (#PCDATA)>
<!ELEMENT heading (#PCDATA)>
<!ELEMENT body (#PCDATA)>
```

```xml
<!DOCTYPE note [
<!ELEMENT note (to, from, heading, body)>
<!ELEMENT to (#PCDATA)>
<!ELEMENT from (#PCDATA)>
<!ELEMENT heading (#PCDATA)>
<!ELEMENT body (#PCDATA)>
]>
```

중심에서 0.3cm 떨어진 소속 18px

DTD

XML

선언	설명
<!ELEMENT>	element의 이름과 구조 정의
<!ATTLIST>	element의 attribute 정의
<!ENTITY>	엔티티를 정의 ☆
<!NOTATION>	데이터의 해석 방식 정의
<!DOCTYPE>	DOCTYPE 정의

Document Type Definition

중심에서 0.3cm 떨어진 소속 18px

XML 실습

XML

선언	설명
<!ELEMENT>	element의 이름과 구조 정의
<!ATTLIST>	element의 attribute 정의
<!ENTITY>	엔티티를 정의 ☆
<!NOTATION>	데이터의 해석 방식 정의
<!DOCTYPE>	DOCTYPE 정의

Document Type Definition

중심에서 0.3cm 떨어진 소속 18px

과제 [Movie time table]

dreamhack.io/wargame/challenges/1887

선언	설명
<!ELEMENT>	element의 이름과 구조 정의
<!ATTLIST>	element의 attribute 정의
<!ENTITY>	엔티티를 정의 ☆
<!NOTATION>	데이터의 해석 방식 정의
<!DOCTYPE>	DOCTYPE 정의

Document Type Definition

중심에서 0.3cm 떨어진 소속 18px

2000.00.00

Q&A

질문이 있다면 하십시오

발표자

2.5cm-3.5cm 떨어진 제목 36px

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

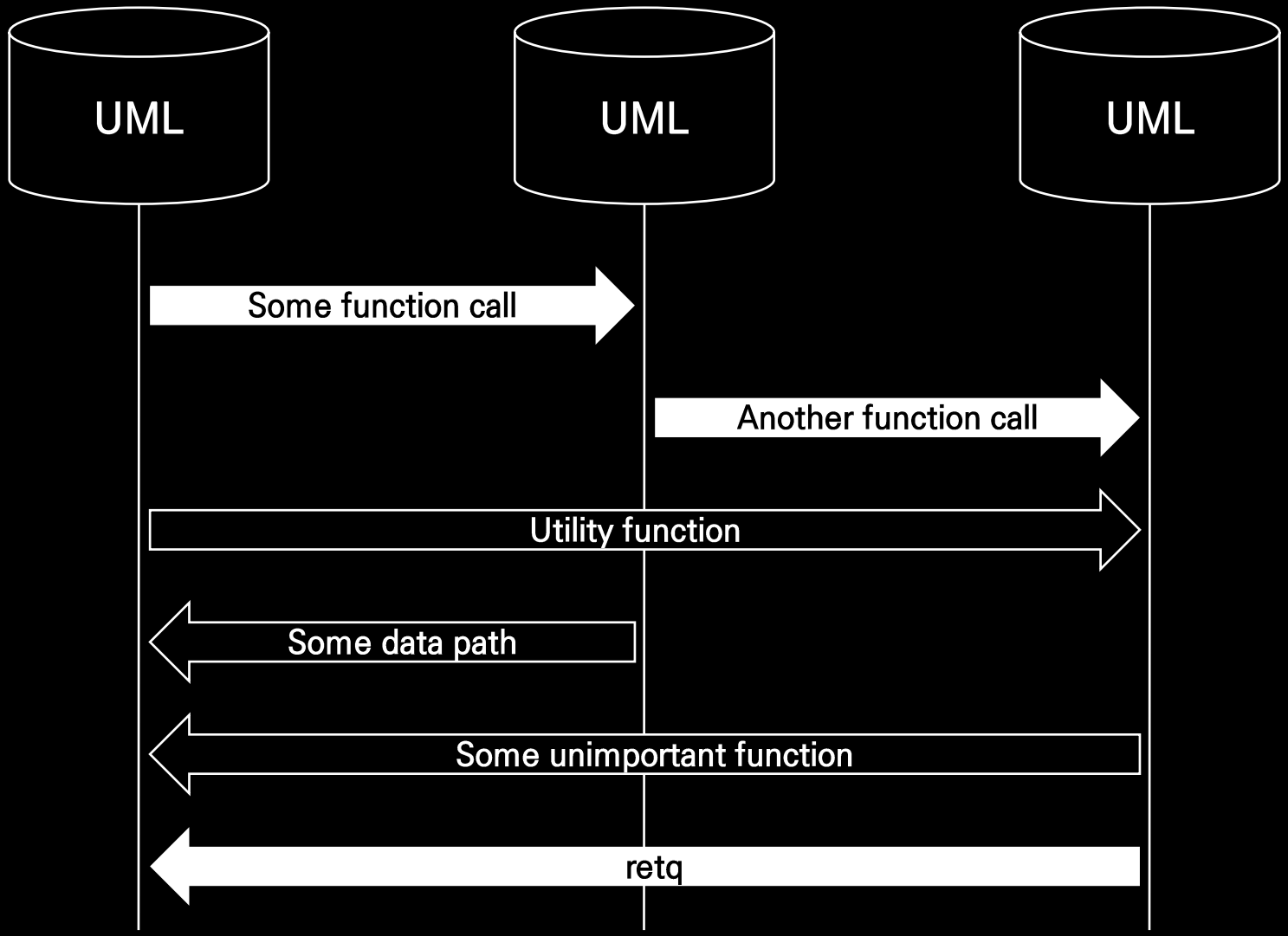
```
Git init
Git status
Git add text.txt
Git add .
Git commit
Ctrl+C
Git commit -m “genesis”
Git log
Git log --oneline
```

```
Git add .
Git reset .
Git commit -m “add README”
Git log --oneline -n 3
Git commit –a –m “hello”
```

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px

중심에서 0.3cm 떨어진 소속 18px



중심에서 0.3cm 떨어진 소속 18px