2000.00.00

Request Forgery

가디언 웹 보안 세미나 5

발표자

Request Forgery

Parameter tampering, IDOR

I

Request Forgery

Concept

Client가 보낼 수 있는 요청

curl, request, burpsuite, …

공격자가 충분히 변조할 수 있다.

유저의 입력을 신뢰하지 말 것!!

중심에서 0.3cm 떨어진 소속 18px

Request Forgery

Exploit - Preview

이전 http 요청을 떠올리자.

"모든" 부분을 변조할 수 있음

Authorization Token도 그 대상

중심에서 0.3cm 떨어진 소속 18px

Parameter tampering

요청에 이상한 값을 넣자

```
/buy?price=50000
```

Client 측 로직을 신뢰한 상황

```
/buy?price=1
```

1원에 살 수 있다.

중심에서 0.3cm 떨어진 소속 18px

Parameter tampering

Q. 신뢰하면 어떻게 되나요?
A. 개인정보를 모두에게 opensource로 제공할 수 있습니다.

곧 배울 IDOR 예시

출처: SBS

중심에서 0.3cm 떨어진 소속 18px

Parameter tampering

Example – php

```php
<?php
$q = $_GET['q'];
echo "You searched for: $q";
?>
```

중심에서 0.3cm 떨어진 소속 18px

Parameter tampering

Example – php

```
[Request]
GET /search?q=<script>alert(1)</script>


[Response]
You searched for: <script>alert(1)</script>
```

XSS

중심에서 0.3cm 떨어진 소속 18px

Request Forgery

Prevention

중요한 정보는 조작이 어렵게!

BE에서 검증절차를 추가하자

중심에서 0.3cm 떨어진 소속 18px

Insecure Direct Object Reference

Concept

`/user?id=24`

id 값만 조작하면?

`/user?id=0`

다른 사람들의 프로필 확인

중심에서 0.3cm 떨어진 소속 18px

Insecure Direct Object Reference

Concept

왜 발생했을까?

Broken Access Control

세션 사용자 != 리소스 주인

중심에서 0.3cm 떨어진 소속 18px

Insecure Direct Object Reference

Prevention

리소스 접근시 권한 검증

UUID 해시 활용

최소 권한 원칙 (Principle of Least Privilege)

사용하는데 최소한의 권한만 부여

중심에서 0.3cm 떨어진 소속 18px

Side Note

Web Application Firewall

입력 값들을 필터링

Known Exploit을 기반으로 필터링

중심에서 0.3cm 떨어진 소속 18px

Server-Side Request Forgery

내부망에서 요청의 변조

II

Local Backend Server

SSRF

중요한 백엔드는 exposed port 없음

Client → FE → BE 구조

FE 와 BE 는 `fetch` 등으로 소통

Local에만 port를 열어둔다.

중심에서 0.3cm 떨어진 소속 18px

Local Backend Server

SSRF

잘 만들었다면?

슬라이드 노트에 적힌 거 말고 있을까?

중심에서 0.3cm 떨어진 소속 18px

SSRF

Vulnerable Example

FE → curl → BE

누가봐도 위험하다!

SSRF 방지가 충분한가?

중심에서 0.3cm 떨어진 소속 18px

SSRF

Exploit

주로 취약한 Filter 또는 Request Method

WA에서 사용한 library에 취약점 존재 가능

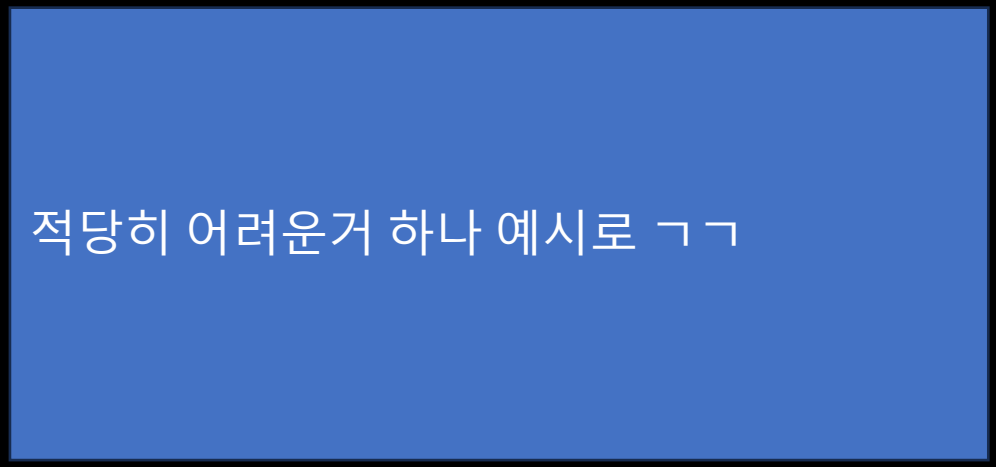
CVE details, Exploit DB를 활용하여 검색

PoC가 없다면 직접 git 커밋 흔적으로 조사한다.

중심에서 0.3cm 떨어진 소속 18px

실습 []

TBD



중심에서 0.3cm 떨어진 소속 18px

Homework [web-ssrf]

dreamhack.io/wargame/challenges/75

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

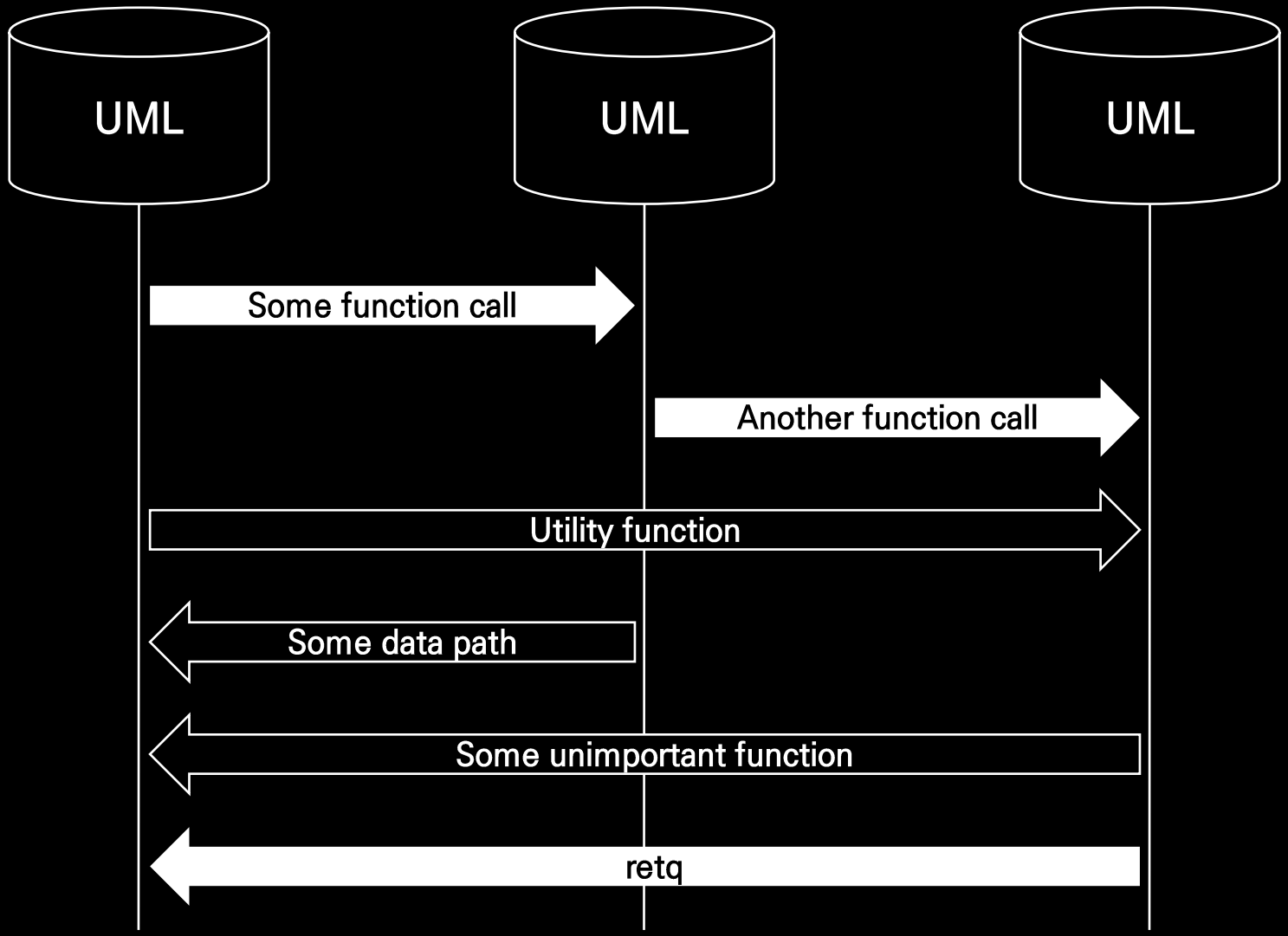
```
Git init
Git status
Git add text.txt
Git add .
Git commit
Ctrl+C
Git commit -m “genesis”
Git log
Git log --oneline
```

```
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

Local Backend Server

SSRF

중요한 백엔드는 exposed port 없음

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

Client →

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