Analysis on new web app attacks

Who Am I?

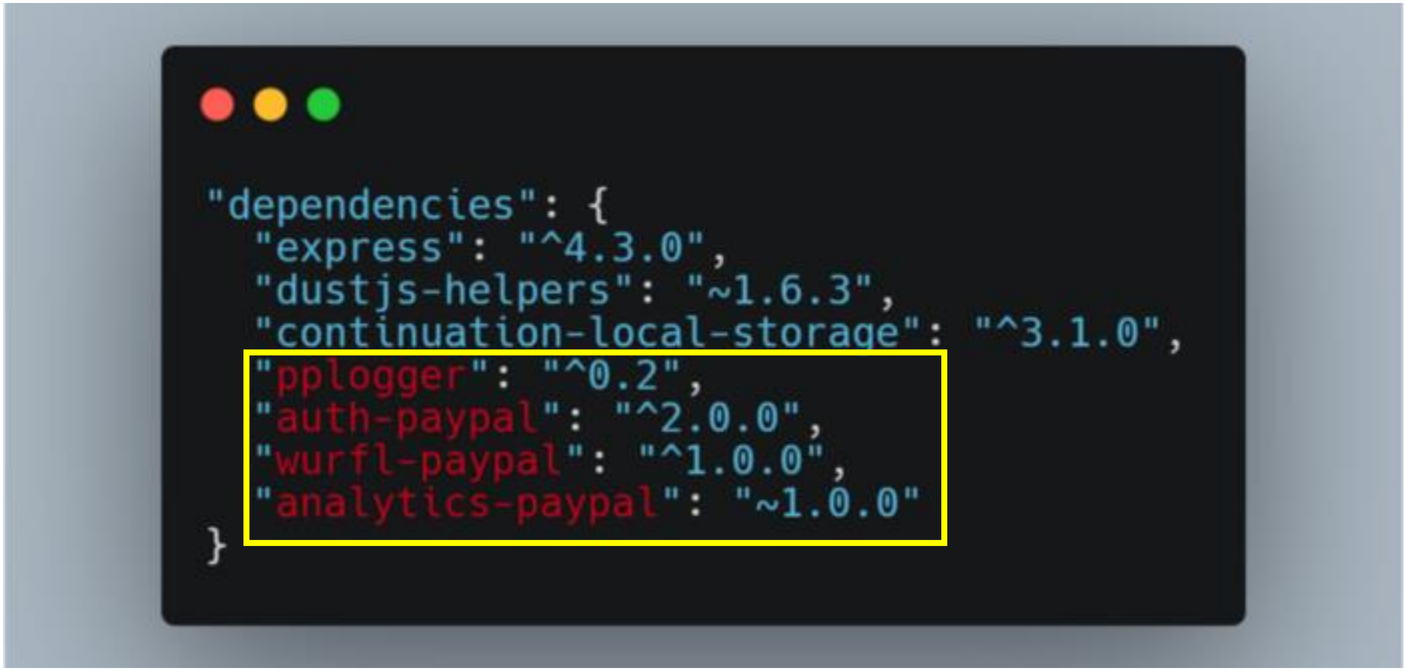
- HaruulZangi
- 6+ years in cyber security
- @Infosolution, Information security analyst

Dependency Confusion

- Alex Birsan
- twitter.com/alxbrsn
- Summer of 2020
- Paypal bug hunt

Dependency Confusion

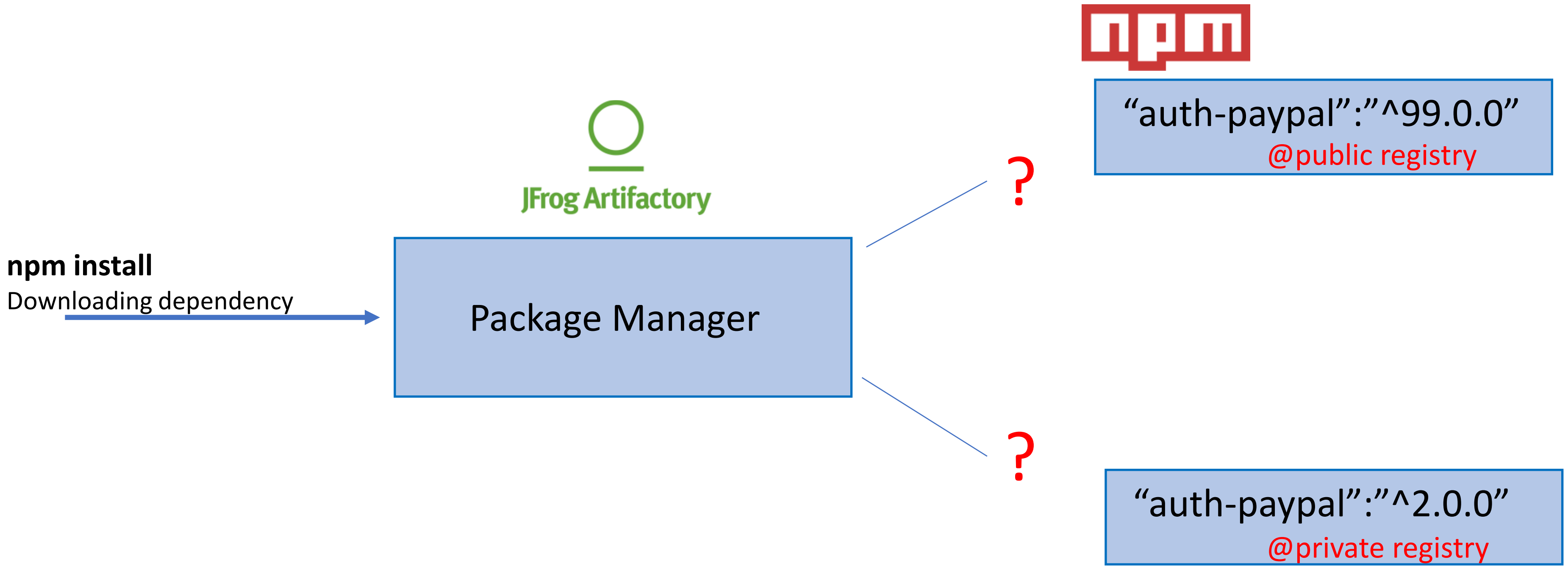
Хэрвээ private dependency-тэй ижил нэртэй package дотор хортой код хийгээд npm дээр байршуулбал яах бэ?



```
"dependencies": {
  "express": "^4.3.0",
  "dustjs-helpers": "~1.6.3",
  "continuation-local-storage": "^3.1.0",
  "pplogger": "^0.2",
  "auth-paypal": "^2.0.0",
  "wurfl-paypal": "^1.0.0",
  "analytics-paypal": "~1.0.0"
}
```

package.json

Dependency Confusion: Root cause



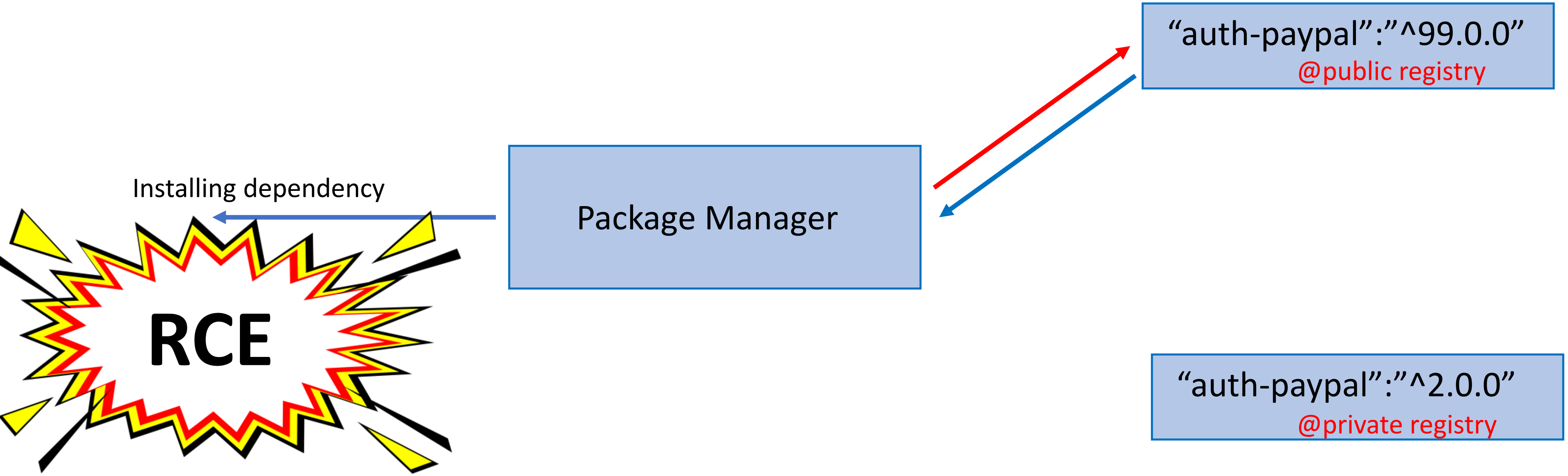
npm install
Downloading dependency

Package Manager

“auth-paypal”:”^99.0.0”
@public registry

“auth-paypal”:”^2.0.0”
@private registry

Dependency Confusion



“auth-paypal”:”^99.0.0”

@public registry

Package Manager

Installing dependency

RCE

“auth-paypal”:”^2.0.0”

@private registry

Dependency Confusion

Хакерууд Private dependency-г хаанаас олж болох вэ?

- JS файл
- Public github repo
- Pastebin
- Лог файлууд

Dependency Confusion

Paypal+Shopify+Tesla+Microsoft+… = $130K bounty

Dependency Confusion: Mitigation

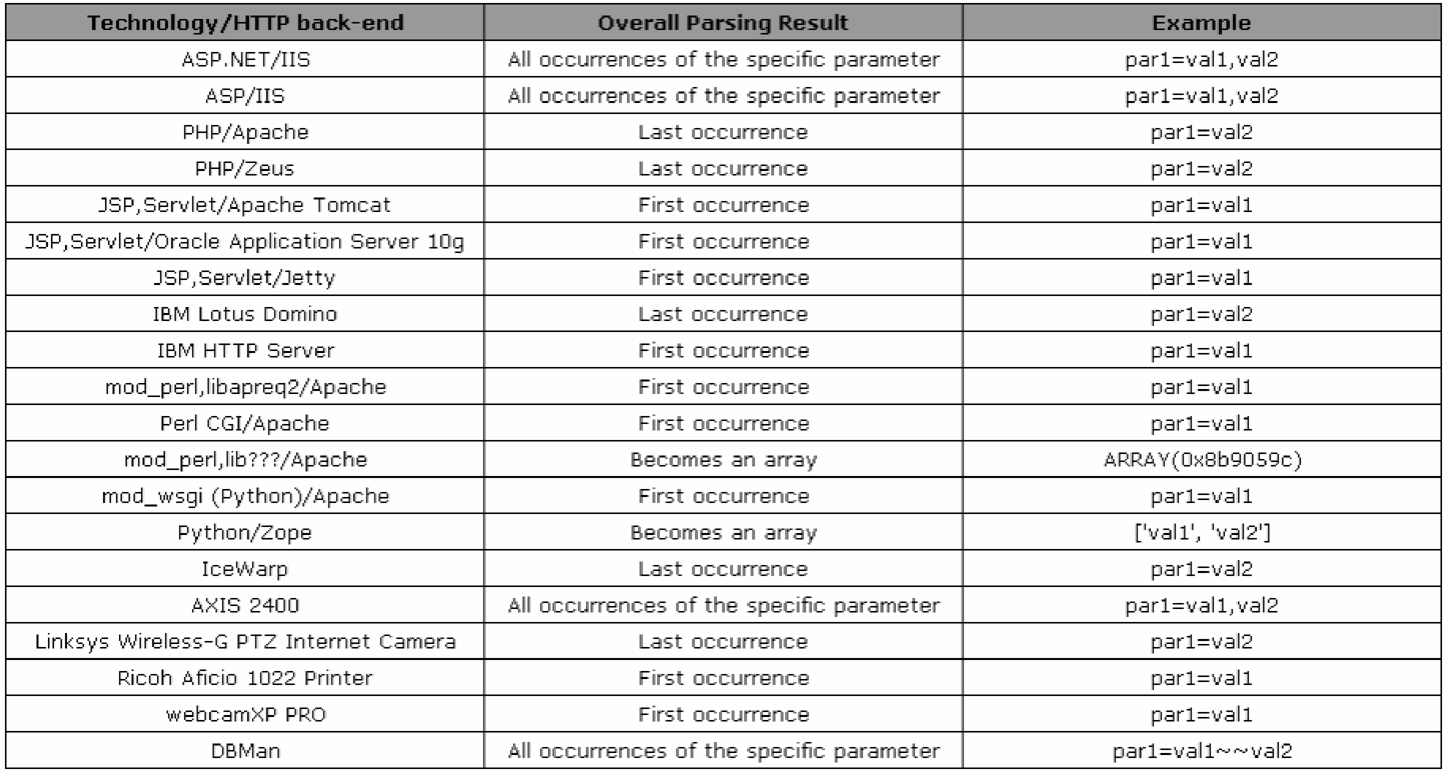
1. Package manager-ээ upgrade хийх
2. Ихэнх package manager-үүдэд байдаг "**scope**"-ыг ашиглах. Жишээлбэл npm дээр scope тохируулаад package-ыг дуудахдаа "@somescope/somepackage" байдлаар дууддаг учраас ижил нэртэй package-тай андуурагдахгүй
3. Dependency-г дуудахдаа яг хувилбараар нь дуудах жишээлбэл "1.5.8" гэх мэт

HTTP Parameter Pollution /HPP/

Ижил нэртэй HTTP параметруудыг зохицуулах ямар нэгэн RPC стандарт байдаггүй учраас web application бүр өөрийнхөөрөө зохицуулалт хийдэг

http://api.example.com/transaction?amount=100&amount=15

HTTP Parameter Pollution /HPP/



Technology/HTTP back-end	Overall Parsing Result	Example
ASP.NET/IIS	All occurrences of the specific parameter	par1=val1,val2
ASP/IIS	All occurrences of the specific parameter	par1=val1,val2
PHP/Apache	Last occurrence	par1=val2
PHP/Zeus	Last occurrence	par1=val2
JSP,Servlet/Apache Tomcat	First occurrence	par1=val1
JSP,Servlet/Oracle Application Server 10g	First occurrence	par1=val1
JSP,Servlet/Jetty	First occurrence	par1=val1
IBM Lotus Domino	Last occurrence	par1=val2
IBM HTTP Server	First occurrence	par1=val1
mod_perl,libapreq2/Apache	First occurrence	par1=val1
Perl CGI/Apache	First occurrence	par1=val1
mod_perl,lib???/Apache	Becomes an array	ARRAY(0x8b9059c)
mod_wsgi (Python)/Apache	First occurrence	par1=val1
Python/Zope	Becomes an array	['val1', 'val2']
IceWarp	Last occurrence	par1=val2
AXIS 2400	All occurrences of the specific parameter	par1=val1,val2
Linksys Wireless-G PTZ Internet Camera	Last occurrence	par1=val2
Ricoh Aficio 1022 Printer	First occurrence	par1=val1
webcamXP PRO	First occurrence	par1=val1
DBMan	All occurrences of the specific parameter	par1=val1~~val2

https://owasp.org/www-pdf-archive/AppsecEU09_CarettoniDiPaola_v0.8.pdf

HPP: Server side

Pollute server side variable

http://bank.com/transaction?to=John&amount=100

Authorization: Bearer eyJhbGciOiJ..

Decode JWT
from=James

http://payment-gateway:8081/transaction?to=John&amount=100&from=James

http://bank.com

Decode JWT
from=Attacker

http://payment-gateway:8081/transaction?to=John&amount=100&from=Victim&from=Attacker

http://bank.com/transaction?to=John&amount=100&from=Victim

Authorization: Bearer eyJhbGciO3J..

HPP: WAF evasion

http://example.com/showproducts.asp?prodID=9 UNION SELECT 1,2,3 FROM Users WHERE id=3 —

WAF prodID=9 UNION SELECT 1,2,3 FROM Users WHERE id=3 — 🚫

---

http://example.com/showproducts.asp?prodID=9 /*&prodID=*/UNION /*&prodID=*/SELECT 1 &prodID=2 &prodID=3 FROM /*&prodID=*/Users /*&prodID=*/ WHERE id=3 —

WAF prodID=9 /* ✓

WAF prodID =*/UNION /* ✓

WAF prodID =*/SELECT 1 ✓

WAF prodID=2 ✓

WAF prodID=3 FROM /* ✓

WAF prodID=*/Users /* ✓

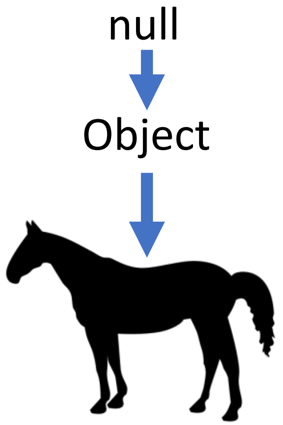
WAF prodID=*/ WHERE id=3 — ✓

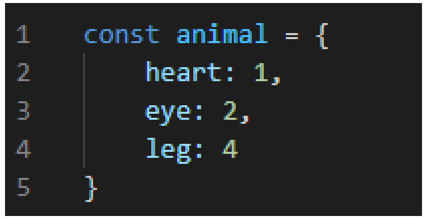
HPP: Mitigation

- GET/POST Парамертрүүдийг back end-рүү дамжуулахын өмнө шалгах. Жнь Regex
- GET/POST параметрыг дамжуулахдаа URL encode хийх
- WAF ашиглах /Comercial or HPP илрүүлэх чадамжтай/

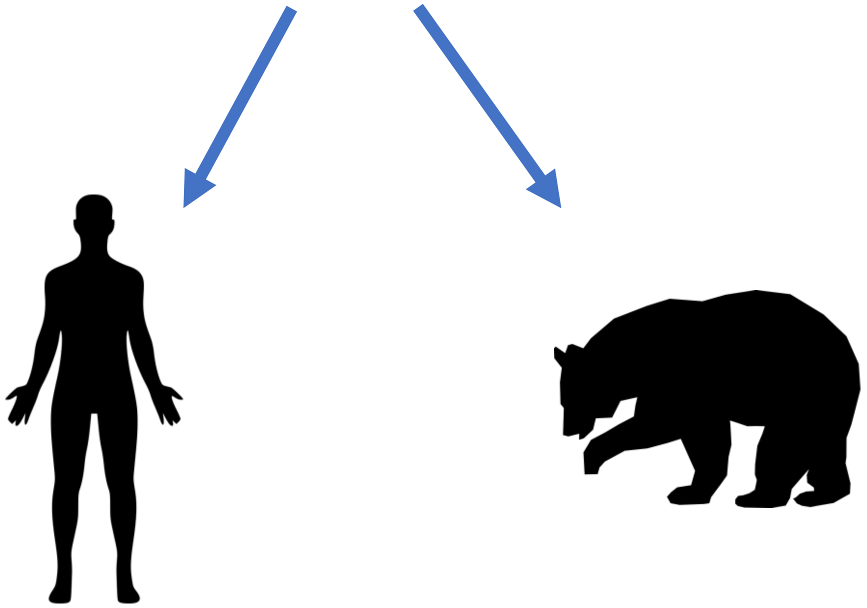
Prototype Pollution

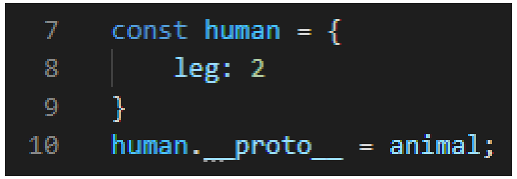
Javascript бол
Prototype удамшил
ашигладаг хэл



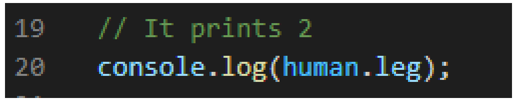


```
const animal = {
    heart: 1,
    eye: 2,
    leg: 4
}
```

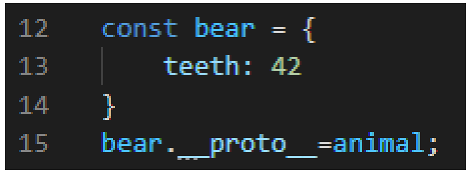




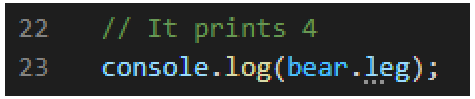
```
const human = {
    leg: 2
}
human.__proto__ = animal;
```



```
// It prints 2
console.log(human.leg);
```



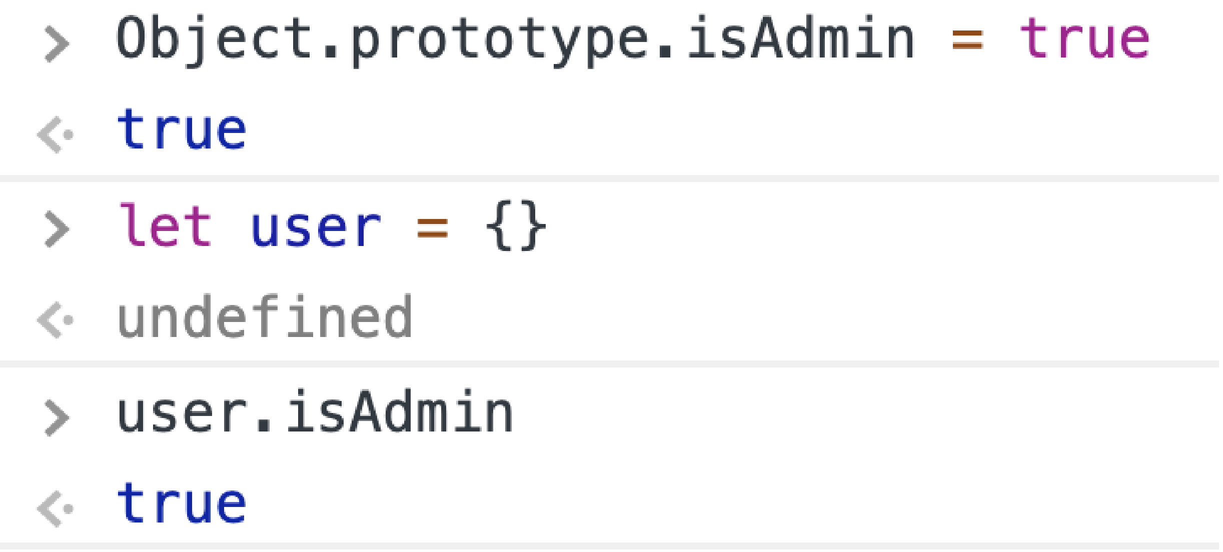
```
const bear = {
    teeth: 42
}
bear.__proto__=animal;
```



```
// It prints 4
console.log(bear.leg);
```

Prototype Pollution

```
if (user.isAdmin) {
        //do something
}
```



```
> Object.prototype.isAdmin = true
< true
> let user = {}
< undefined
> user.isAdmin
< true
```

Prototype Pollution

DEMO

Prototype Pollution

```
testObject.__proto__.polluted = true
testObject.prototype.polluted = true
testObject.constructor.prototype.polluted = true
```

Prototype Pollution: Mitigation

- Upgrade merge package
- Schema validation of JSON input
- Use Map instead of Object
- Object.create(null) let test = Object.create(animal)

Асуулт/Хариулт