The API Assessment Primer

Jason Haddix & Greg Patton

OWASP AppSecEU | May 21, 2015

OWASP AppSecEU 15
Amsterdam, The Netherlands

Agenda

- Introduction
- Why API security matters
- Assessment considerations
- Common API vulnerabilities
- Takeaways

About me

Greg Patton
SAST Manager, HP Fortify on Demand

- Manage the static analysis testing team for HP FoD
- Nearly ten years of DAST experience with web & mobile apps
- Attended my 1st OWASP meeting on June 7, 2007 (Houston, TX)

hacker@hp.com

Why API Security Matters

APIs are everywhere

- Mobile apps
- Internet of Things (IoT)
- Service Oriented Architecture (soa)
- Enterprise thick-client apps

API insecurity

- New surface area = dangerous surface area
- Many API developers haven’t had security training
- Many assume that because back ends aren’t visited by end-users they are more secure (obscurity assumption)

API insecurity

Most APIs are vulnerable

- Analyzing any given API is likely to yield significant vulnerabilities
- The newer, more eager the shop – the higher the chance of issues

API Assessment Considerations

API testing approach

- Acquire information
- Map the API
- Capture runtime traffic
- Use automated scanners
- Manually test, test, test

What to collect pre-assessment

Ask customer for

- Source code
  - Static analysis & review
- Documentation
  - Regular user
  - Admin documentation
- Valid request data
  - Known-good param values
  - Order of function calls

Core toolset

Web proxy / HTTP editor

- ZAP proxy
- BURP suite pro

Network capture tools

- Wireshark
- Echo Mirage

Web service testing tools

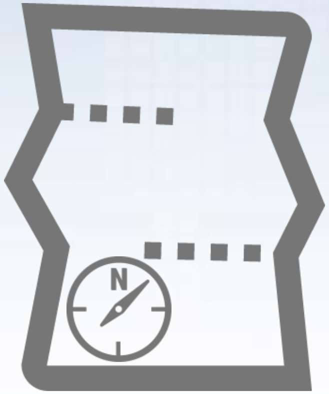
- SoapUI
- WSAttacker
- HP WebInspect
- Postman

Browser extensions

- Chrome: Advanced Rest Client
- Firefox: Hackbar

API Mapping

Fully map the API, listing all methods and functionality at the start of an assessment



Examine:

- asmx
- /help & help docs
- WSDL (.NET)
- WADL (Java)
- Doxegen & help docs

Google

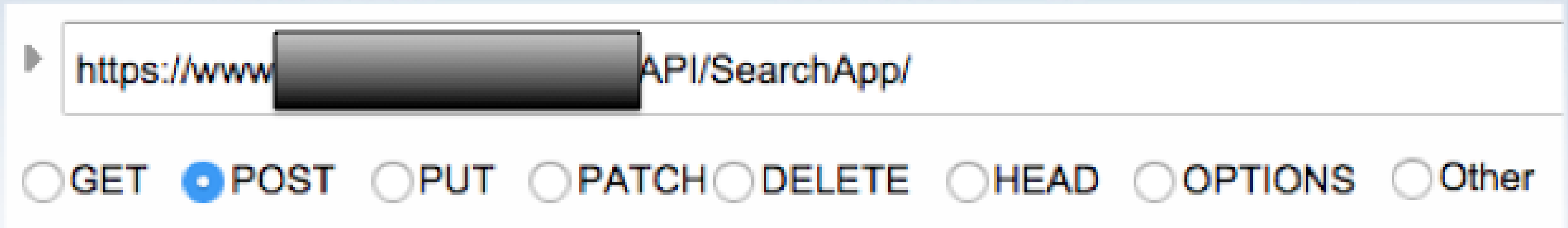
- inurl:wsdl site:example.com

Explore

- runtime operations

API Mapping | Testing

Try different HTTP Methods



https://www[redacted]API/SearchApp/

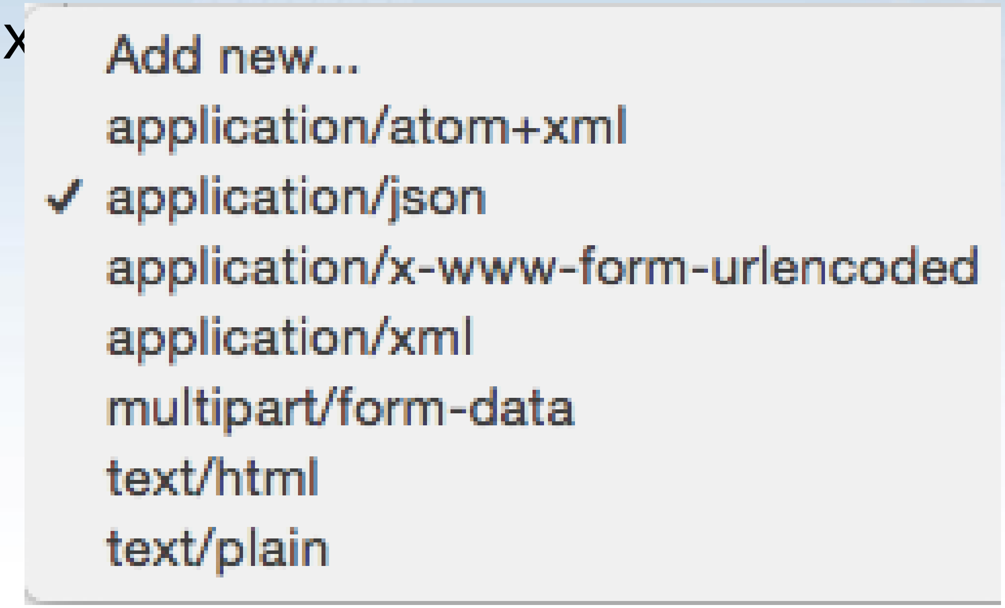
○ GET ● POST ○ PUT ○ PATCH ○ DELETE ○ HEAD ○ OPTIONS ○ Other

- Don’t assume other verbs won’t work
- May discover hidden functionality

API Mapping | Testing

Try different content types and executions

- JSON vs. XML vs. Tex
- REST vs. XML



Add new...
application/atom+xml
✓ application/json
application/x-www-form-urlencoded
application/xml
multipart/form-data
text/html
text/plain

Common API Vulnerabilities

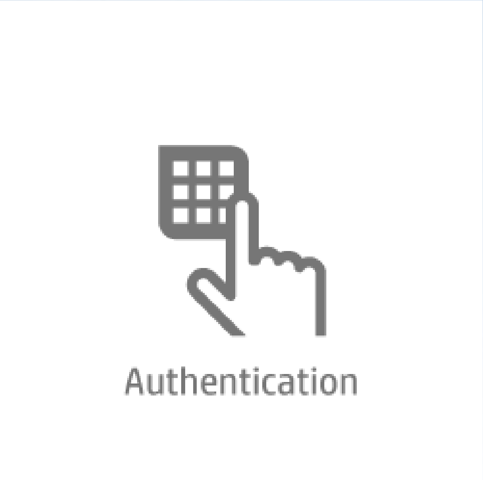
Common API Vulnerabilities

- Broken Authentication & Session Management
- Information Leakage
- Not-So-Hidden Functionality
- Lack of Access Control
- Tampering & Trust Flaws
- Lack of Insecure Transport
- Injection Flaws
- Failure to Protect Keys

Authentication & Session | Concerns

- No authentication
- Insecure framework implementation
  - openID
  - oAuth
- Non-expiring session tokens
- Weak password complexity
- Lack of account lockout
- Lack of logout/session expiration mechanism

Authentication & Session | Testing



- Attempt to send requests with no authentication
- Review authentication scheme or framework
- Attempt to use simple passwords
- Attempt to use old session tokens
- Verify logout functionality truly expires sessions
- Weak password complexity
- Attempt to lock account

Authentication & Session | Protections

- Require authentication
- Require strong password
- Use up-to-date frameworks
  - Latest version of oAuth, etc.
- Ensure there is a way to logout / expire sessions
- Pay special attention to sensitive operations
- Use rate limiting to guard again Brute Force abuse

Information Leakage | Concerns

Often APIs respond with more data than required

- Apps returning all records instead of only needed or requested records
  - Particularly common in mobile applications
- Lack of data limiters
  - No limits on the number of requests a user can send
  - Brute force all records

Information Leakage | Concerns

2014 RSA Mobile App - Exposed Personal Data

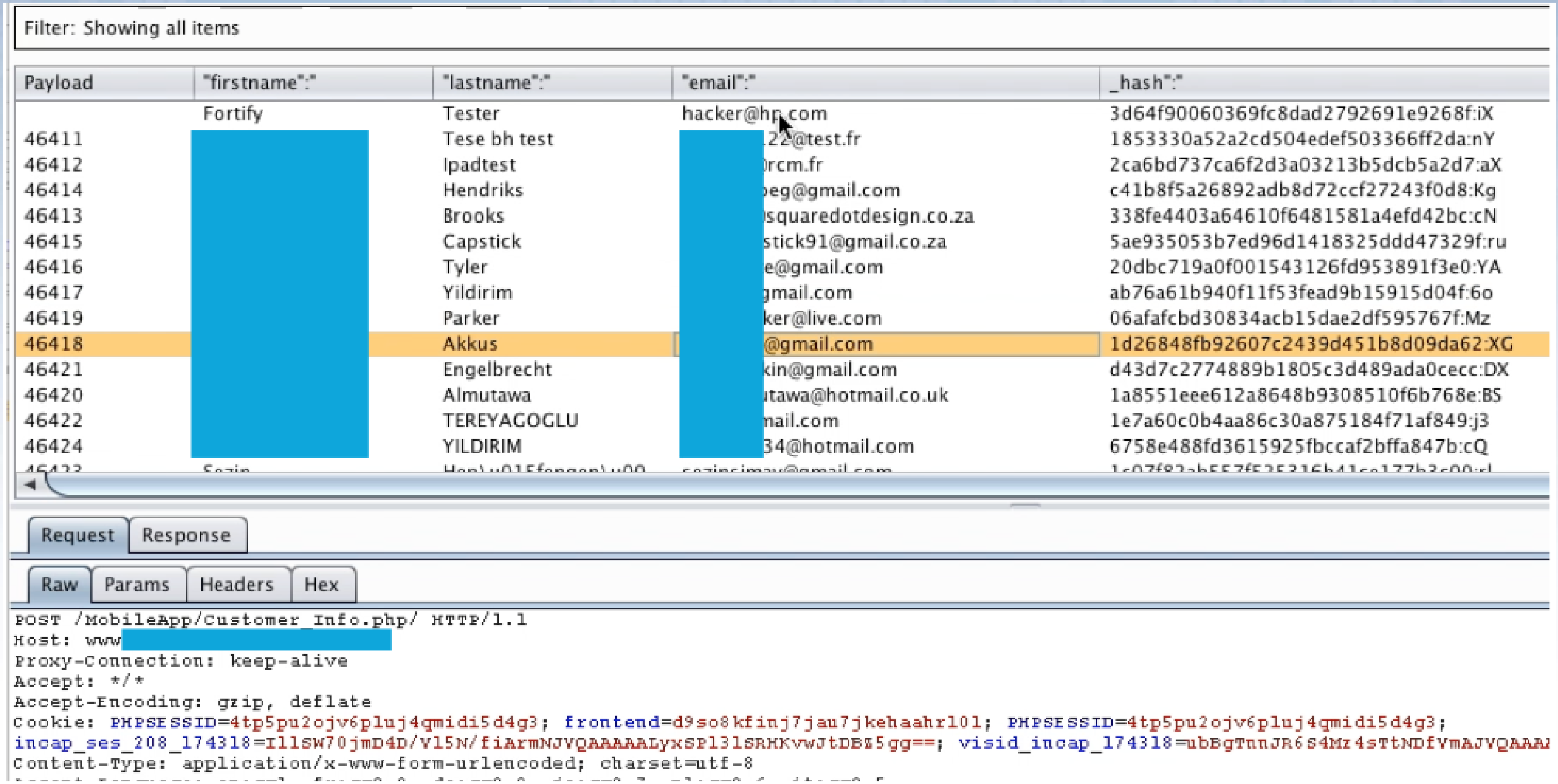
- App designed for connecting with conference activities, viewing schedules, venue maps, etc.
- App used a web API to download information about every registered user of the application

- http://blog.ioactive.com/2014/02/beware-your-rsa-mobile-app-download.html

Information Leakage | Testing

- Review API responses
  - Do they return more data than what was requested?
- Try wildcard values
  - * , %, ?, space, etc.
- Review error messages
  - Do they reveal technical information?
  - Do they reveal enumeration flaws?

Information Leakage | Testing



Filter: Showing all items

Payload	"firstname":"	"lastname":"	"email":"	_hash":"
	Fortify	Tester	hacker@hp.com	3d64f90060369fc8dad2792691e9268f:iX
46411	[redacted]	Tese bh test	[redacted]22@test.fr	1853330a52a2cd504edef503366ff2da:nY
46412	[redacted]	Ipadtest	[redacted]rcm.fr	2ca6bd737ca6f2d3a03213b5dcb5a2d7:aX
46414	[redacted]	Hendriks	[redacted]eg@gmail.com	c41b8f5a26892adb8d72ccf27243f0d8:Kg
46413	[redacted]	Brooks	[redacted]squaredotdesign.co.za	338fe4403a64610f6481581a4efd42bc:cN
46415	[redacted]	Capstick	[redacted]stick91@gmail.co.za	5ae935053b7ed96d1418325ddd47329f:ru
46416	[redacted]	Tyler	[redacted]e@gmail.com	20dbc719a0f001543126fd953891f3e0:YA
46417	[redacted]	Yildirim	[redacted]gmail.com	ab76a61b940f11f53fead9b15915d04f:6o
46419	[redacted]	Parker	[redacted]ker@live.com	06afafcbd30834acb15dae2df595767f:Mz
46418	[redacted]	Akkus	[redacted]@gmail.com	1d26848fb92607c2439d451b8d09da62:XG
46421	[redacted]	Engelbrecht	[redacted]kin@gmail.com	d43d7c2774889b1805c3d489ada0cecc:DX
46420	[redacted]	Almutawa	[redacted]tawa@hotmail.co.uk	1a8551eee612a8648b9308510f6b768e:BS
46422	[redacted]	TEREYAGOGLU	[redacted]mail.com	1e7a60c0b4aa86c30a875184f71af849:j3
46424	[redacted]	YILDIRIM	[redacted]34@hotmail.com	6758e488fd3615925fbccaf2bffa847b:cQ
46423	Sezin	Han\u015fengen\u00	sezinsimay@gmail.com	1c07f82ab557f525316b41ce177b3c00:rl

```
POST /MobileApp/Customer_Info.php/ HTTP/1.1
Host: www[redacted]
Proxy-Connection: keep-alive
Accept: */*
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=4tp5pu2ojv6pluj4qmidi5d4g3; frontend=d9so8kfinj7jau7jkehaahrl01; PHPSESSID=4tp5pu2ojv6pluj4qmidi5d4g3;
incap_ses_208_174318=I1lSW70jmD4D/Vl5N/fiArmNJVQAAAAALyxSPl3lSRHKvwJtDBZ5gg==; visid_incap_174318=ubBgTnnJR6S4Mz4sTtNDfVmAJVQAAAA
Content-Type: application/x-www-form-urlencoded; charset=utf-8
```

Information Leakage | Protections

- Only return requested & needed data
- Review responses for sensitive information
- Review error messages

Hidden functionality | Concerns

API hidden functionality flaws are largely introduced due to faulty developer assumptions, i.e. not thinking like an attacker

- assume obscurity
- assume users will use functions only as intended

Hidden functionality | Testing

- Test different HTTP verbs
  - GET, POST, PUT, DELETE, etc.
- Check for API verbs
  - edit user, add user, delete user
- Review WSDLs, etc. for functionality not called at runtime
- Fuzz to find hidden operations
  - https://www.owasp.org/index.php/**OWASP_SecLists_Project**

Hidden functionality | Protections

- Ensure only required methods are exposed
- Ensure authentication scheme protects sensitive functions

Lack of access controls | Concerns

APIs don’t always verify the requestor is authorized for the target object

- Indirect Object References

Tampering & trust | Concerns

- Tampering with commands
  - Bypass client-side controls
  - Tampering with queries
- Incoming & outgoing data
- Malicious upload/download

Lack of access controls Tampering & trust | Testing

Intercept & modify requests

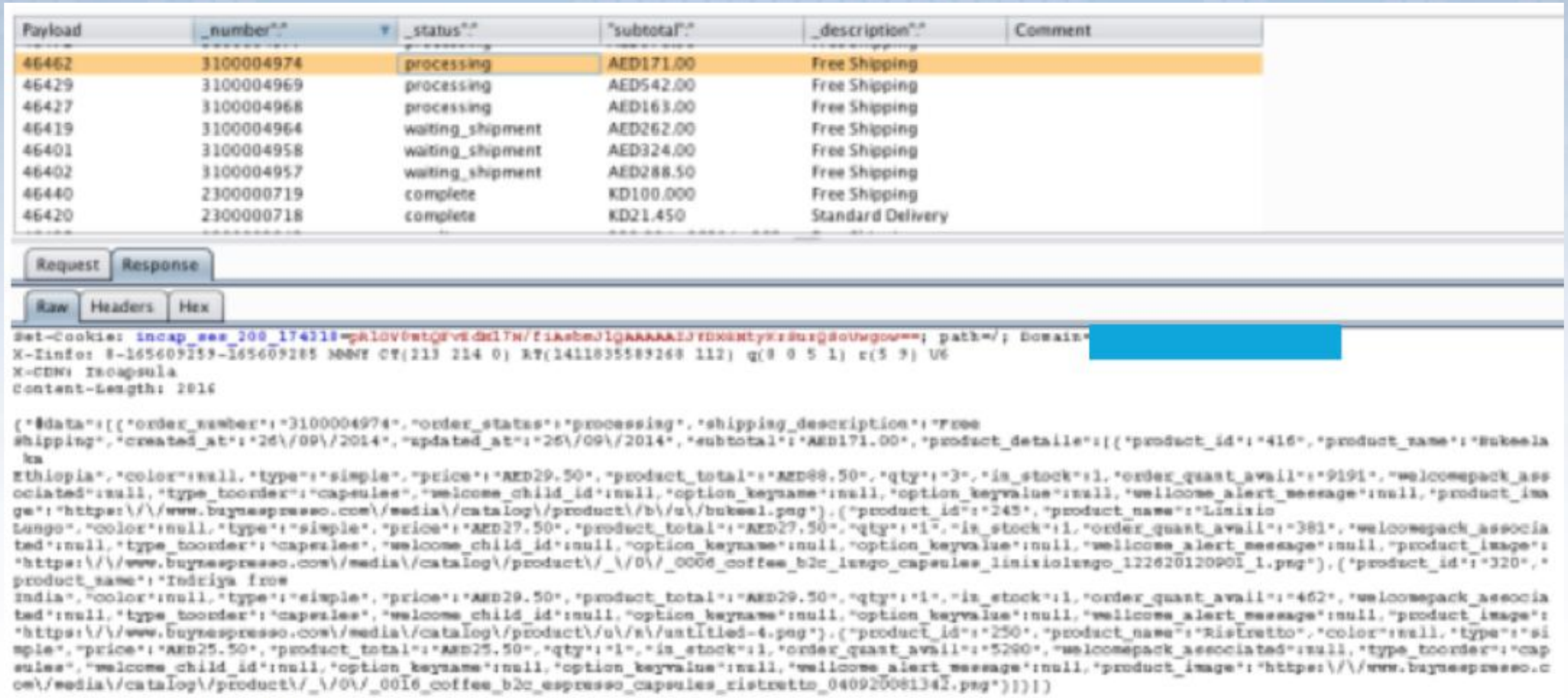
- Modify parameters to attempt to access other data
  - Account numbers, User IDs, Order numbers, etc.

Intercept & modify responses

- Change the content available in mobile apps
- Bypass controls

Lack of access controls | Testing

Tampering & trust



Payload	_number":"	_status":"	"subtotal":"	_description":"	Comment
46462	3100004974	processing	AED171.00	Free Shipping	
46429	3100004969	processing	AED542.00	Free Shipping	
46427	3100004968	processing	AED163.00	Free Shipping	
46419	3100004964	waiting_shipment	AED262.00	Free Shipping	
46401	3100004958	waiting_shipment	AED324.00	Free Shipping	
46402	3100004957	waiting_shipment	AED288.50	Free Shipping	
46440	2300000719	complete	KD100.000	Free Shipping	
46420	2300000718	complete	KD21.450	Standard Delivery	

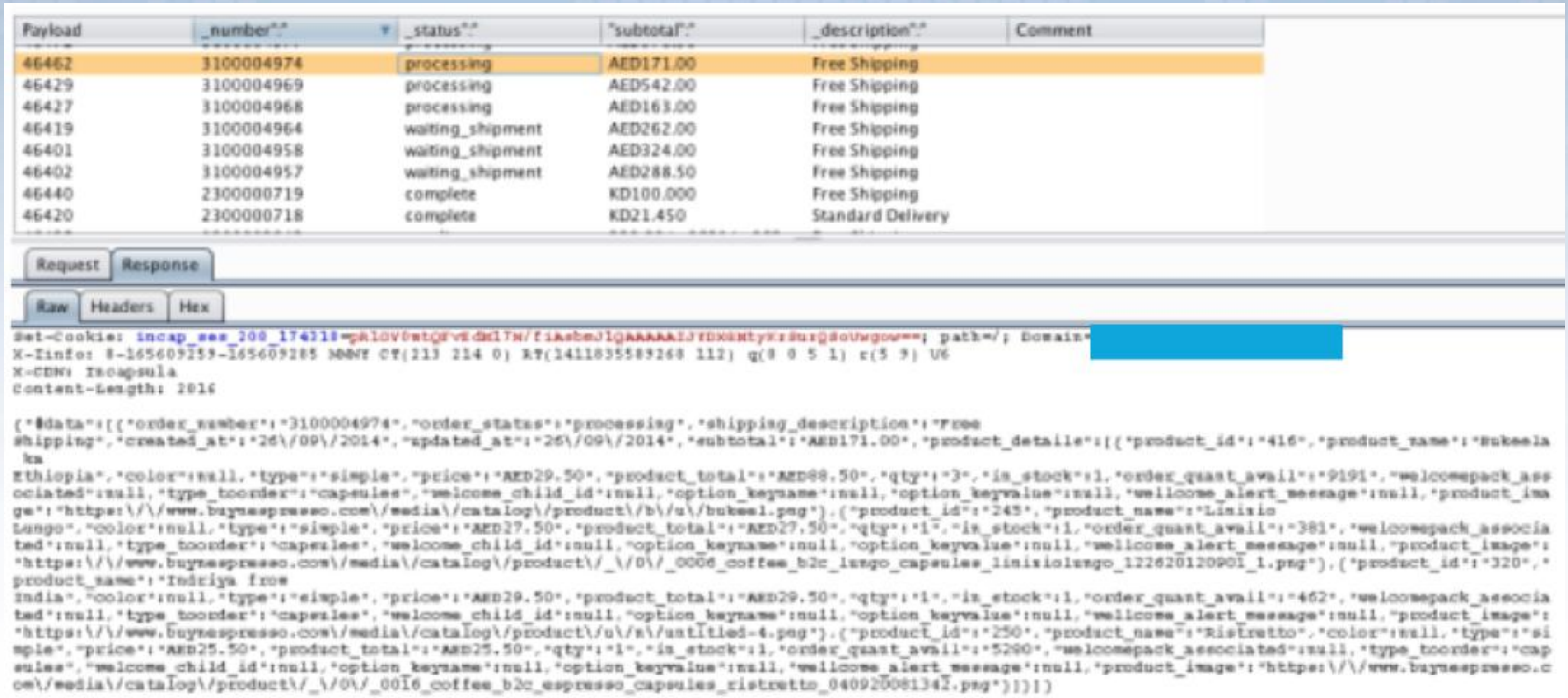
```
Set-Cookie: incap_ses_200_174318=pAlOV0mtQFvEdMlTN/fiAsbeJlQAAAAAIJfDXENtyKzSurQdoUwgow==; path=/; Domain=[redacted]
X-Iinfo: 8-165609259-165609285 NNNY CT(213 214 0) RT(1411835589268 112) q(0 0 5 1) r(5 9) U6
X-CDN: Incapsula
Content-Length: 2016

{"#data":[{"order_number":"3100004974","order_status":"processing","shipping_description":"Free
Shipping","created_at":"26\/09\/2014","updated_at":"26\/09\/2014","subtotal":"AED171.00","product_details":[{"product_id":"416","product_name":"Bukeela
 ka
Ethiopia","color":null,"type":"simple","price":"AED29.50","product_total":"AED88.50","qty":"3","in_stock":1,"order_quant_avail":"9191","welcomepack_ass
ociated":null,"type_toorder":"capsules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_ima
ge":"https:\/\/www.buynespresso.com\/media\/catalog\/product\/b\/u\/bukeel.png"},{"product_id":"245","product_name":"Linizio
Lungo","color":null,"type":"simple","price":"AED27.50","product_total":"AED27.50","qty":"1","in_stock":1,"order_quant_avail":"381","welcomepack_associa
ted":null,"type_toorder":"capsules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_image":
"https:\/\/www.buynespresso.com\/media\/catalog\/product\/_\/0\/_0006_coffee_b2c_lungo_capsules_liniziolungo_122620120901_1.png"},{"product_id":"320","
product_name":"Indriya from
India","color":null,"type":"simple","price":"AED29.50","product_total":"AED29.50","qty":"1","in_stock":1,"order_quant_avail":"462","welcomepack_associa
ted":null,"type_toorder":"capsules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_image":
"https:\/\/www.buynespresso.com\/media\/catalog\/product\/u\/n\/untitled-4.png"},{"product_id":"250","product_name":"Ristretto","color":null,"type":"si
mple","price":"AED25.50","product_total":"AED25.50","qty":"1","in_stock":1,"order_quant_avail":"5290","welcomepack_associated":null,"type_toorder":"cap
sules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_image":"https:\/\/www.buynespresso.c
om\/media\/catalog\/product\/_\/0\/_0016_coffee_b2c_espresso_capsules_ristretto_040920081342.png"}]}]}
```

Enumeration of User Orders

OWASP AppSecEU 15
Amsterdam, The Netherlands

Lack of access controls Tampering & trust | Testing



Payload	_number":"	_status":"	"subtotal":"	_description":"	Comment
46462	3100004974	processing	AED171.00	Free Shipping	
46429	3100004969	processing	AED542.00	Free Shipping	
46427	3100004968	processing	AED163.00	Free Shipping	
46419	3100004964	waiting_shipment	AED262.00	Free Shipping	
46401	3100004958	waiting_shipment	AED324.00	Free Shipping	
46402	3100004957	waiting_shipment	AED288.50	Free Shipping	
46440	2300000719	complete	KD100.000	Free Shipping	
46420	2300000718	complete	KD21.450	Standard Delivery	

```
Set-Cookie: incap_ses_200_174318=pA1OVOmtQFvEdMlTN/fiAsbeJ1gAAAAAIJYDXHNtyKrHurQdoUwgow==; path=/; Domain=[redacted]
X-Iinfo: 8-165609259-165609285 NNNY CT(213 214 0) RT(1411835589268 112) q(0 0 5 1) r(5 9) U6
X-CDN: Incapsula
Content-Length: 2016

{"@data":[{"order_number":"3100004974","order_status":"processing","shipping_description":"Free
Shipping","created_at":"26\/09\/2014","updated_at":"26\/09\/2014","subtotal":"AED171.00","product_details":[{"product_id":"416","product_name":"Bukeela
 ka
Ethiopia","color":null,"type":"simple","price":"AED29.50","product_total":"AED88.50","qty":"3","in_stock":1,"order_quant_avail":"9191","welcomepack_ass
ociated":null,"type_toorder":"capsules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_ima
ge":"https:\/\/www.buynespresso.com\/media\/catalog\/product\/b\/u\/bukeel.png"},{"product_id":"245","product_name":"Linizio
Lungo","color":null,"type":"simple","price":"AED27.50","product_total":"AED27.50","qty":"1","in_stock":1,"order_quant_avail":"381","welcomepack_associa
ted":null,"type_toorder":"capsules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_image":
"https:\/\/www.buynespresso.com\/media\/catalog\/product\/_\/0\/_0006_coffee_b2c_lungo_capsules_linizіolungo_122620120901_1.png"},{"product_id":"320","
product_name":"Indriya from
India","color":null,"type":"simple","price":"AED29.50","product_total":"AED29.50","qty":"1","in_stock":1,"order_quant_avail":"462","welcomepack_associa
ted":null,"type_toorder":"capsules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_image":
"https:\/\/www.buynespresso.com\/media\/catalog\/product\/u\/n\/untitled-4.png"},{"product_id":"250","product_name":"Ristretto","color":null,"type":"si
mple","price":"AED25.50","product_total":"AED25.50","qty":"1","in_stock":1,"order_quant_avail":"5290","welcomepack_associated":null,"type_toorder":"cap
sules","welcome_child_id":null,"option_keyname":null,"option_keyvalue":null,"wellcome_alert_message":null,"product_image":"https:\/\/www.buynespresso.c
om\/media\/catalog\/product\/_\/0\/_0016_coffee_b2c_espresso_capsules_ristretto_040920081342.png"}]}]}
```

Enumeration of User Orders

Lack of access controls Tampering & trust | Protections

- Validate Parameters
- Test for proper protection of sensitive information
- Review who has access to sensitive information
- Ensure only authorized users have access to sensitive information

OWASP AppSecEU 15
Amsterdam, The Netherlands

Transport security flaws | Concerns

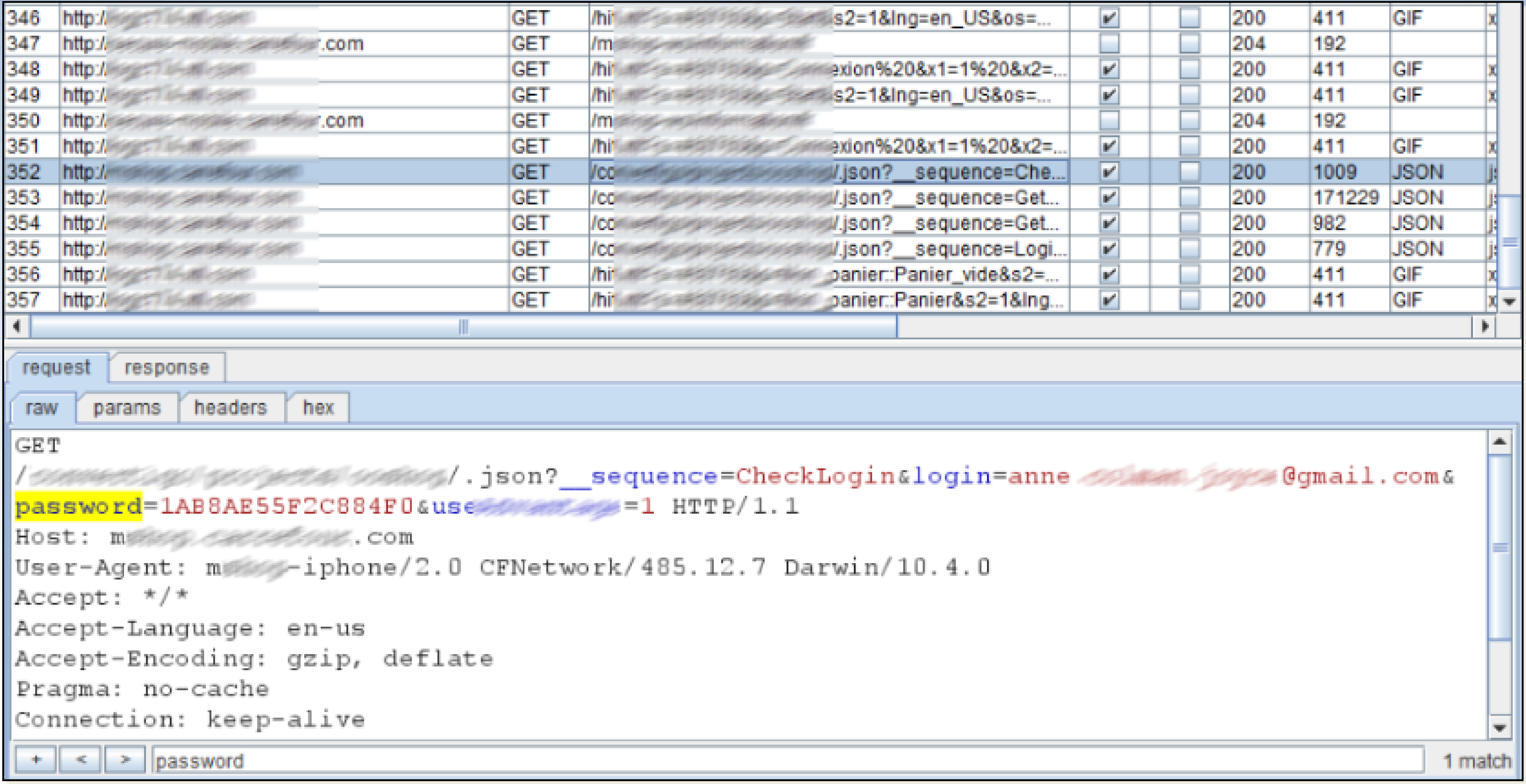
APIs often lack sufficient protection of confidentiality and integrity of data in transit.

- Devices connected to untrustworthy networks
- Sensitive data transmitted in clear-text
  - No encryption
  - Encryption not enforced
- Poorly implemented SSL/TLS

Transport security flaws | Testing

- Review network traffic
- Check for cipher flaws & versions
  - SSLdigger, SSLScan, & other SSL testing tools

Transport security | Testing



346	http:/[redacted]	GET	/hi[redacted]s2=1&lng=en_US&os=...	☑	☐	200	411	GIF	x
347	http:/[redacted].com	GET	/m[redacted]	☐	☐	204	192		
348	http:/[redacted]	GET	/hi[redacted]exion%20&x1=1%20&x2=...	☑	☐	200	411	GIF	x
349	http:/[redacted]	GET	/hi[redacted]s2=1&lng=en_US&os=...	☑	☐	200	411	GIF	x
350	http:/[redacted].com	GET	/m[redacted]	☐	☐	204	192		
351	http:/[redacted]	GET	/hi[redacted]exion%20&x1=1%20&x2=...	☑	☐	200	411	GIF	x
352	http:/[redacted]	GET	/co[redacted]/.json?__sequence=Che...	☑	☐	200	1009	JSON	j:
353	http:/[redacted]	GET	/co[redacted]/.json?__sequence=Get...	☑	☐	200	171229	JSON	j:
354	http:/[redacted]	GET	/co[redacted]/.json?__sequence=Get...	☑	☐	200	982	JSON	j:
355	http:/[redacted]	GET	/co[redacted]/.json?__sequence=Logi...	☑	☐	200	779	JSON	j:
356	http:/[redacted]	GET	/hi[redacted]panier::Panier_vide&s2=...	☑	☐	200	411	GIF	x
357	http:/[redacted]	GET	/hi[redacted]panier::Panier&s2=1&lng...	☑	☐	200	411	GIF	x

```
GET
/[redacted]/.json?__sequence=CheckLogin&login=anne[redacted]@gmail.com&
password=1AB8AE55F2C884F0&use[redacted]=1 HTTP/1.1
Host: m[redacted].com
User-Agent: m[redacted]-iphone/2.0 CFNetwork/485.12.7 Darwin/10.4.0
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Pragma: no-cache
Connection: keep-alive
```

Transport security | Protections

Ensure data is protected in transit

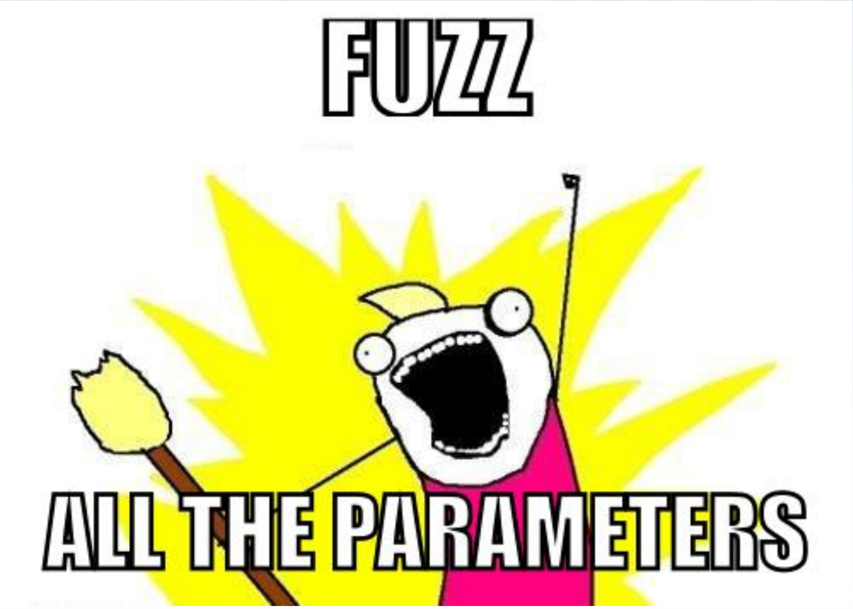
- Ensure sensitive data is never transmitted in clear-text
- Turn on and enforce transport encryption
  - HTTPS everywhere

Injection | Concerns

- SQL injection
- Cross-site sciprting
- Xpath injection
- XML DoS
- XXE – XML external entity

Injection | Testing

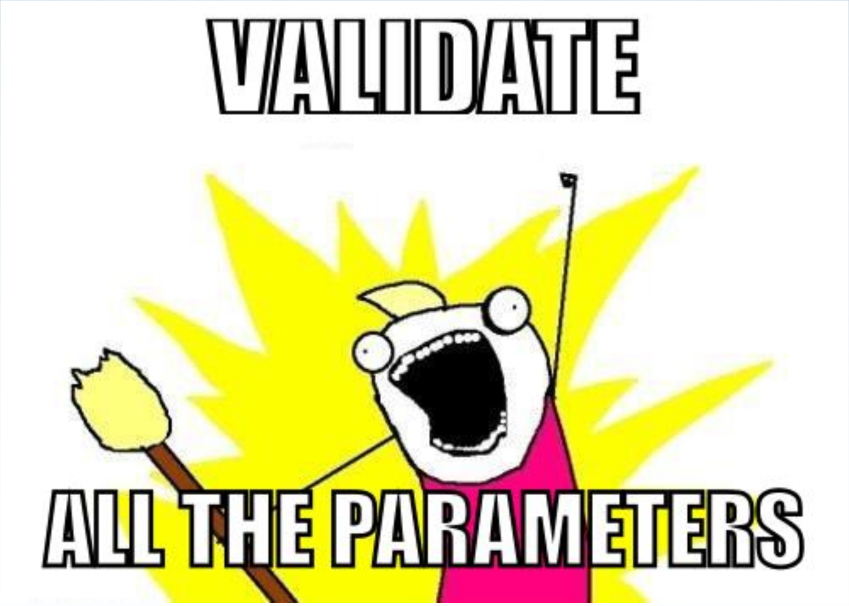
- **Fuzz all parameters**
- Utilize web scanners
- Manually tamper with requests
- Fuzz parameters and review results
- https://www.owasp.org/index.php/Projects/**OWASP_SecLists_Project**



OWASP AppSecEU 15
Amsterdam, The Netherlands

Injection | Protections

- **Validate all parameters** server-side before generating output
- Do not assume clients will adhere to the API specifications



Key Management | Concerns

- Mobile app binaries
  - hardcoded
  - in manifest & .plist files
- Thick-client apps
- Online source code repositories
  - GitHub, BitBucket, etc.

$2375 Mistake

- Developer accidentally uploaded Amazon S3 keys to GitHub
  - Took them down & deleted all traces within 5 minutes
- Automated bot searching for API keys found them
- Amazon API allows users to spin up EC2 instances
- $2375 bill overnight

http://www.devfactor.net/2014/12/30/2375-amazon-mistake/

- Similar Amazon WS story

https://securosis.com/blog/my-500-cloud-security-screwup

Key Management | Testing

- Search for API keys
- Review online source code repositories for API Keys
- Run Strings on binaries & GREP for keys
- Review mobile binaries
  - Manifest files
  - .plist files
  - SQLite Databases

Key Management | Protections

“Keys should be kept under a fake (virtual) rock outside your front door.” – R. Grosse

OWASP AppSecEU 15
Amsterdam, The Netherlands

Takeaways

Takeaways

Adopt the attacker mindset

- Think like an attacker while evaluating your own APIs
- Identify places that developers likely made assumptions
- Attempt to take advantage of those assumptions
- As a developer, think in terms of ***abuse*** vs. just regular *use*

Takeaways

Go with an absolute least-privilege approach

- Do not expose any operations that are not needed
- Do not expose any data that is not required

Takeaways

Leverage available resources

- https://www.owasp.org
- **OWASP IoT Top 10**
  - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project
- **OWASP Mobile Security Project**
  - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

OWASP
The Open Web Application Security Project

OWASP AppSecEU 15
Amsterdam, The Netherlands

Reach out

Greg Patton

hacker@hp.com

http://hp.com/go/fortifyondemand

OWASP AppSecEU 15
Amsterdam, The Netherlands