Broken Access Control Testing (MFLAC, IDOR, ++)

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Bugcrowd University

bugcrowd.com

Module Trainer

- Jason Haddix - @jhaddix
- VP of Trust and Security @Bugcrowd
- Father, hacker, blogger, gamer!

PLAYERUNKNOWN'S BATTLEGROUNDS

Module Outline

1. Module Reading
2. Introduction to IDOR
3. Prominent use cases (public POC’s)
4. Tooling
5. BOSS Labs
6. Resources and References

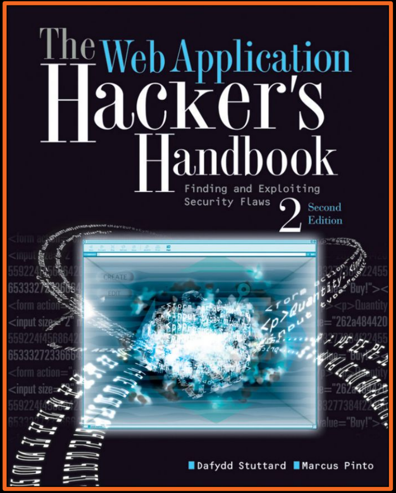
Module Reading

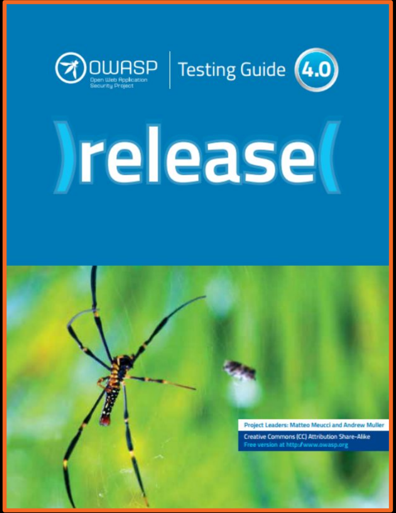
The Web Application Hacker Handbook (2nd Ed)

- Chapter 8 - Attacking Access Controls

The OWASP Testing Guide v4.0

- 4.6.2 Testing for bypassing authorization schema (OTG-AUTHZ-002)
- 4.6.3 Testing for Privilege Escalation (OTG-AUTHZ-003)
- 4.6.4 Testing for Insecure Direct Object References (OTG-AUTHZ-004)




OWASP Open Web Application Security Project
Testing Guide 4.0
)release(
Project Leaders: Matteo Meucci and Andrew Muller
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

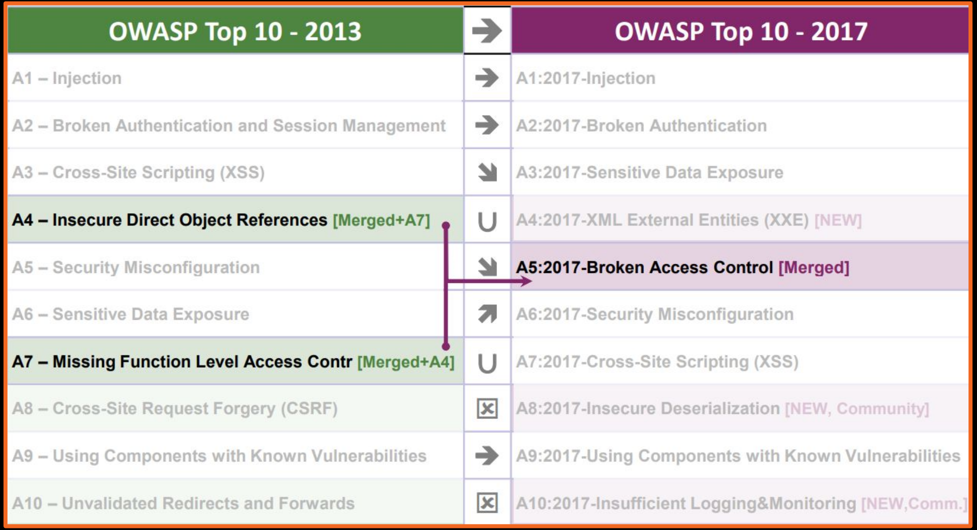
Introduction

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

                # Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Introduction to Access Control bugs

Also known as / related:

- Insecure Direct Object Reference (IDOR)
- Missing Function Level Access Control (MFLAC)
- Privilege Escalation / Authorization Bypass
- Business Logic Flaws
- Forceful Browsing
- Parameter Manipulation
- Path traversal
- Local File Include



OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	**A5:2017-Broken Access Control** [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Simple numeric IDOR

This is the most obvious incarnation of this bug. A function (usually called with a parameter) is passed a numeric value. Because this function lacks access controls you can change this numeric identifier and retrieve data that does not belong to you.

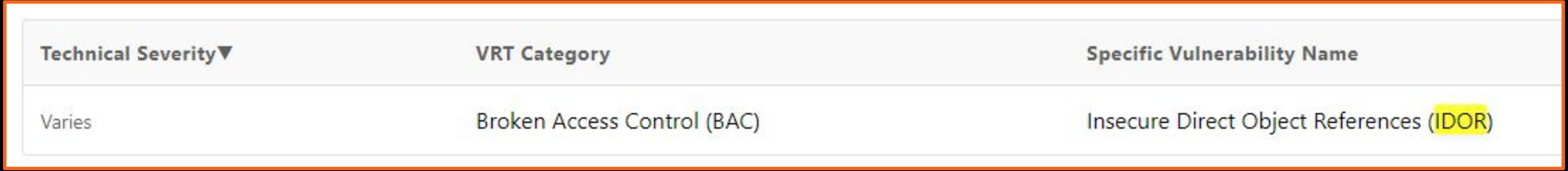
Example

https://www.acme.com/orders/id?=43976

change to

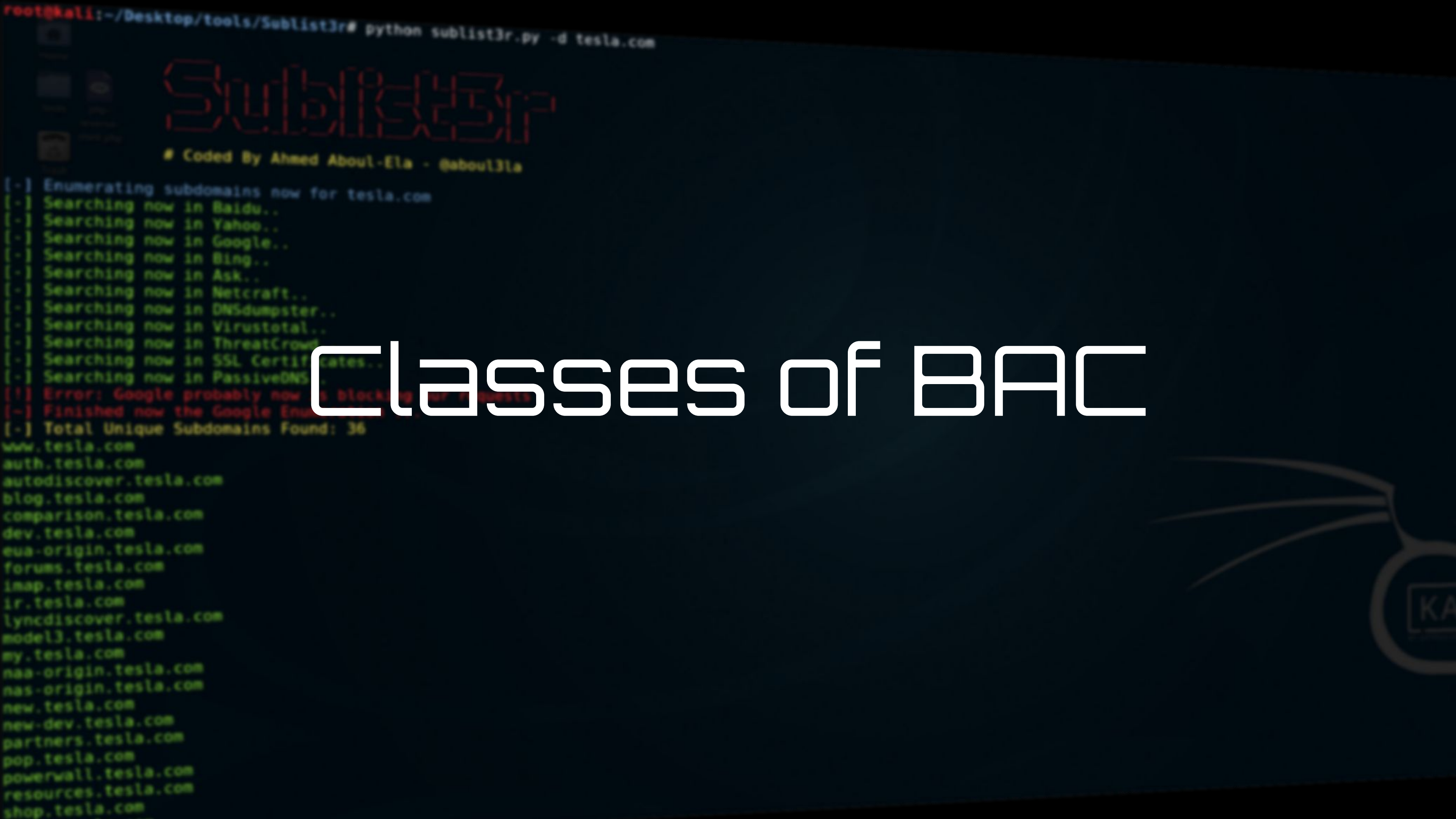
https://www.acme.com/orders/id?=43975

Bugcrowd VRT Rating



Technical Severity▼	VRT Category	Specific Vulnerability Name
Varies	Broken Access Control (BAC)	Insecure Direct Object References (IDOR)

Priority and payouts are largely based on what the function does and what financial impact that function has on the program owner.



Classes of BAC

IDOR in POST

Here is an example of finding a POST request for a function that might be susceptible to IDOR, can you guess where to iterate?

Example

```
POST /account/deleteaccnt HTTP/1.1
Host: acme.com
Connection: close
Content-Length: 22
Cache-Control: max-age=0
Origin: https://acme.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=32145367543634l4df3142gf2341

acID=4321&action=Delete
```

GUID based IDOR

This incarnation of this bug falls under a variant called “missing function level access control”

This request has a unenumerable GUID.

Example

Browsing with account #1 you encounter:

```
https://www.acme.com/changepw/id?=13d573e8-5210-408a-aa77-6e2e9993d264
```

You can then create a 2nd account and you get assigned:

```
https://www.acme.com/changepw/id?=cec4d0ff-f133-4ffd-9ed9-3e0d0c5a3990
```

If you completely log out and log into account #1 and issue the request with the GUID from account #2 you may be able to change that accounts password. Having to find users GUIDs lowers the priority a bit, but look for other endpoints that might allow you to search for a user's GUID!

GUID based IDOR (cont.)

To enumerate GUIDs or non-enumerable account ID's look for other endpoints or web services that might return this data. A quick "search" in your proxy history for your ID should be requests you inspect first and attempt to tamper with to get other IDs (sometimes this can be a vulnerability by itself).

Many times there exists endpoints that will translate you users email into your UUID, these functions sometimes can be used to get another user's GUID. So can search engine scraping, and looking through functions of any associated mobile application. Mobile API's often return verbose levels of data. It is also pertinent to truly verify the UUID or ID is random. Sometimes ID's that seem complex only have portions of them that are random, making them easy to iterate upon.

```
GET /api/data/admin@acme.com HTTP/1.1
Host: acme.com
Connection: close
Content-Length: 22
Cache-Control: max-age=0
Origin: https://acme.com
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Type: text/json; charset=UTF-8
<... SNIPPED ...>


{"accountdata":{"account":"admin@acme.com"},{"uuid":"cec4d0ff-f
133-4ffd-9ed9-3e0d0c5a3990"},{"name":"admin"},{"role":"admin"}}
```

Hash based IDOR

IDOR function values can take many forms. String based, hashed, encoded, etc.

This example is MD5 hashed.

Example

```
POST /account/updatepasswd HTTP/1.1
Host: acme.com
Connection: close
Content-Length: 22
Cache-Control: max-age=0
Origin: https://acme.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=3214536754363414df3142gf2341

userid=912134131a7b11f2dfee0b92bf6b0eed&action=updatepasswd
```

Request methods

When trying to exercise a function pay close attention to what HTTP method is used.

Many REST APIs use PUT or PATCH.

Also notice here the target is an email.

How would you log into this account after IDOR'ing this function?

Example

```
PUT /account/updateEmail HTTP/1.1
Host: acme.com
Connection: close
Content-Length: 22
Cache-Control: max-age=0
Origin: https://acme.com
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=32145367543634l4df3142gf2341

{"accountdata":{"account":"bughunter@bughunter.com"},{"oldEmail":"bughunter
@bughunter.com"},{"newEmail":"badguy@badguy.com"}}
```

Static pages & “forceful browsing”

Many times applications have administrative backends. Sometimes they are behind logins. Many times though a tester can directly access a view/page with sensitive data that is not account specific by just “forcefully browsing” to it.

In some cases these pages might be protected with things like .htaccess files or access rulesets. These can be subject to misconfiguration or bypass.

Example

```
GET /admin/viewTransactions

Access Denied
```

```
GET /ADMIN/viewTransactions

Access granted
```

Static files

Sometimes static files are also subject to access control failures.

Images and documents are key to secure when they deal with private data.

Example

```
GET /patientImages/3216647.jpg
GET /patientDocuments/21714.pdf
```

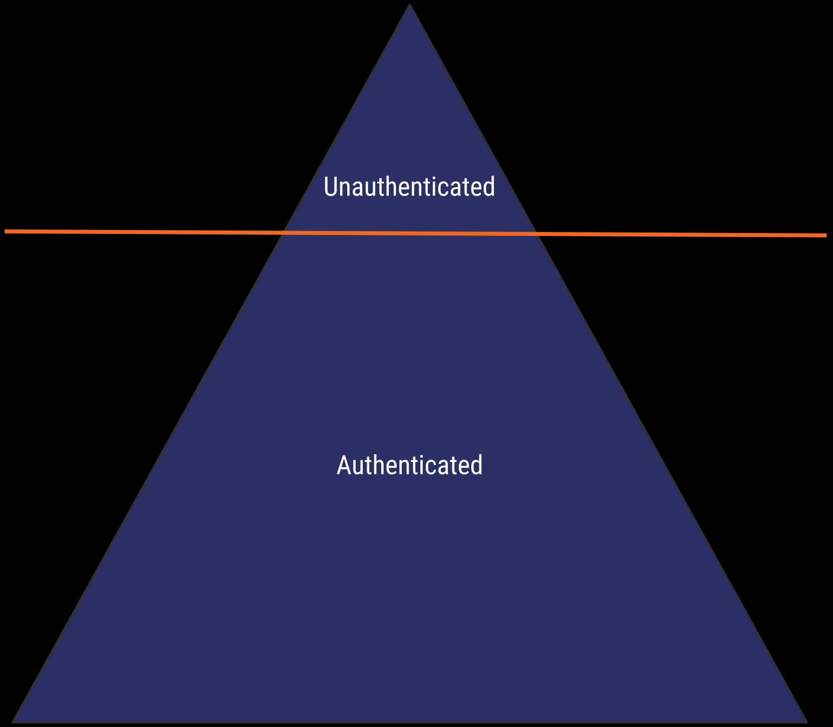
Tooling and Tips

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Auxiliary Tips

Many times the most critical IDORs and MFLAC are only uncovered in the deepest parts of the application.

To find this type of vulnerability you need to make yourself a power user of the application and what it does.



Likely parameters/keyword to check for IDOR

Statistically speaking these are pretty common parameters, REST path names, keywords, and functions associated IDOR and MFLAC.

id	user	Numeric values in parameters under 10 digits REST numeric paths
account	number	
order	no	
doc	key	Functions: Change email Change password Upgrade/downgrade user role View/edit/delete/create context specific app data Shipping, invoices, and document viewing
email	group	
profile	edit	

COTS, OSS, and paywalled applications

Often when testing an application you might identify it is a purchased (Common off the shelf) application, Open Source, or licensed Software.

Investment in installing the application yourself to map out any roles and functions you do not have access to on the client’s hosted site can yield tremendous results.

If the applications is COTS or paywalled, a small investmentment may be worth it.

Sometimes you can gain this knowledge by RTFM or requesting a demo from the software creator/licensor.

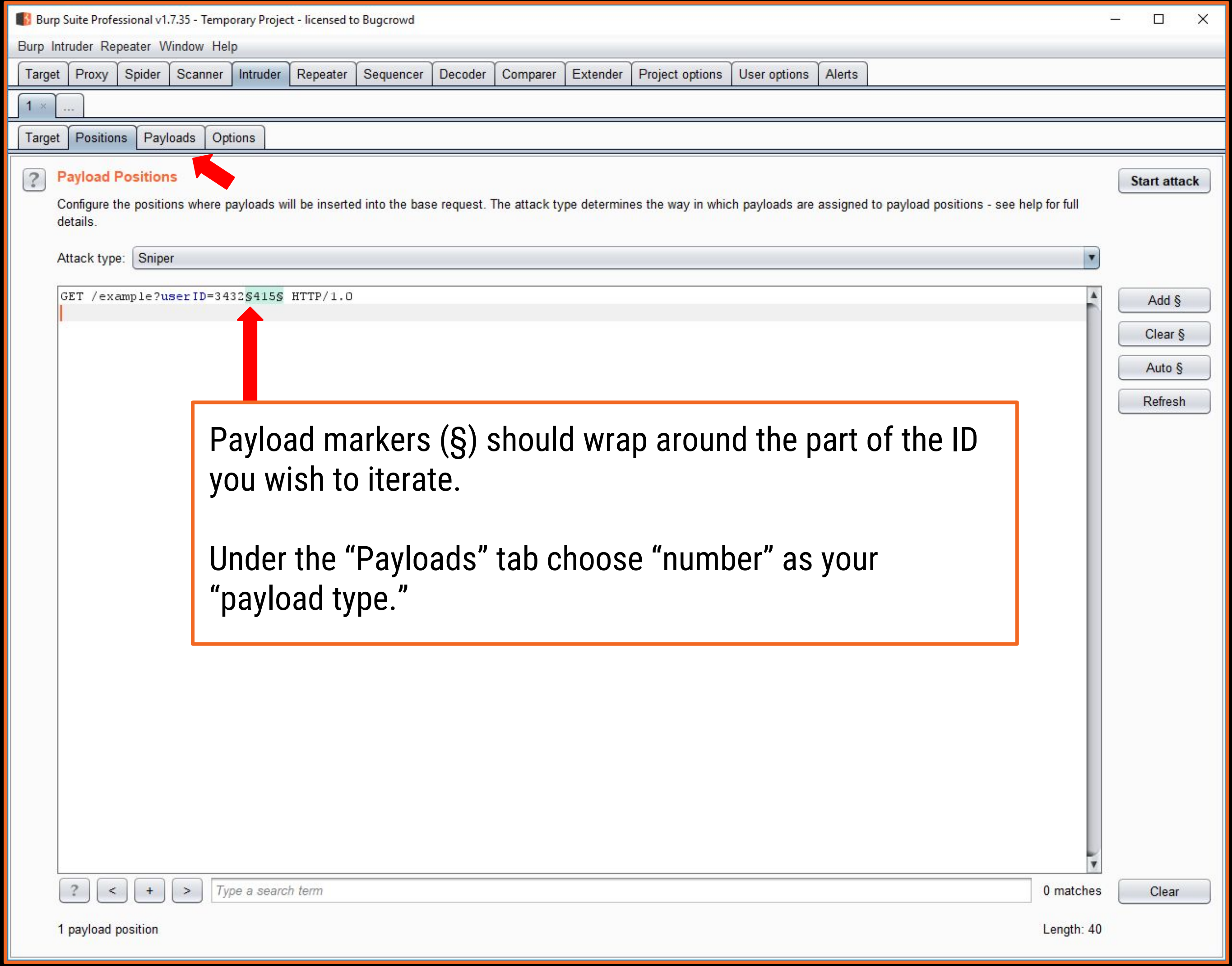
Create a function matrix for MFLAC

When testing for MFLAC it can be useful to create matrix of app functions and who should have the ability to exercise them.

	Update Password	Update Email	Change Account Data	Upgrade Account to Admin	View Logs
Admin	Yes	Yes	Yes	Yes	Yes
User	Yes	Yes	No	No	No
Unauthenticated	No	No	No	No	No

Burp Intruder

For iteration and exploitation of most IDORs Burp Suite's Intruder is used.


Burp Suite Professional v1.7.35 - Temporary Project - licensed to Bugcrowd
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
? < + >
Type a search term
0 matches
Clear

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /example?userID=3432§415§ HTTP/1.0
```

1 payload position

Length: 40

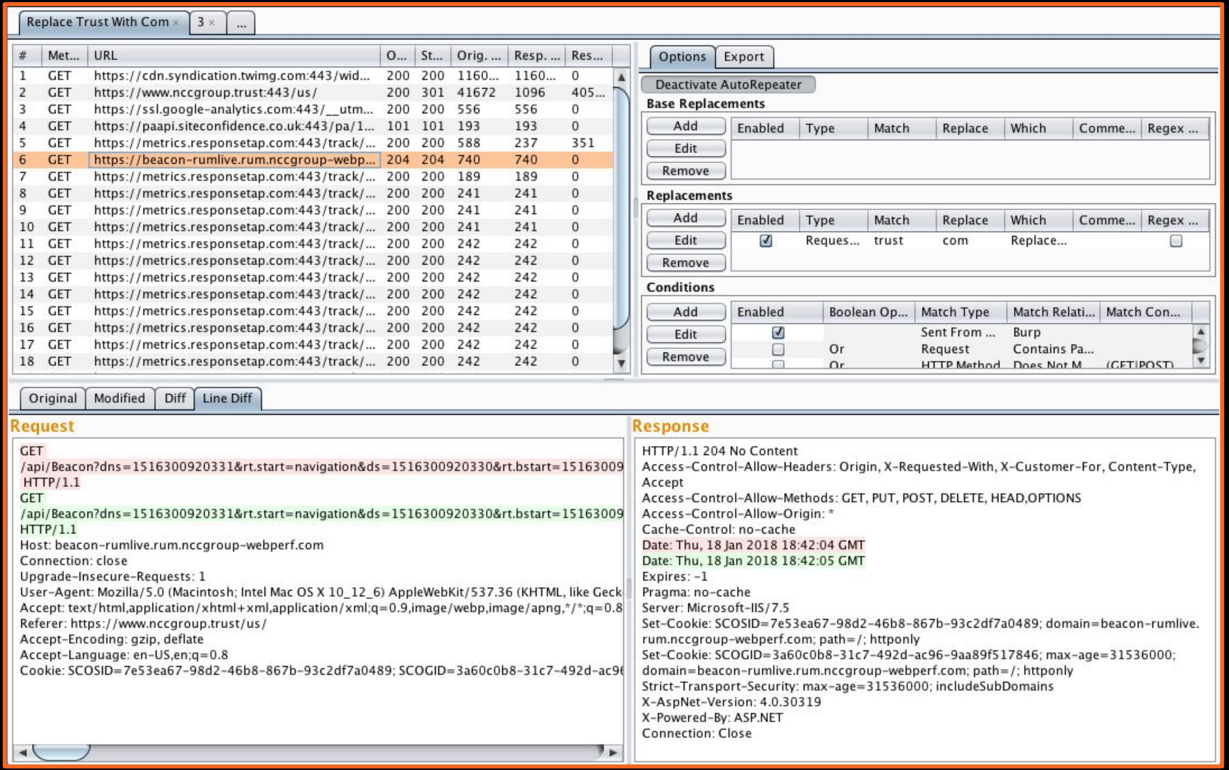
Payload markers (§) should wrap around the part of the ID you wish to iterate.

Under the "Payloads" tab choose "number" as your "payload type."

AuthMatrix, Authz, Autorize, & AutoRepeater

There are several Burp Extensions that can be download via the BApp store for Access Control testing.

All have distinct user interfaces and advantages.



#	Met...	URL	O...	St...	Orig. ...	Resp. ...	Res...
1	GET	https://cdn.syndication.twimg.com:443/wid...	200	200	1160...	1160...	0
2	GET	https://www.nccgroup.trust:443/us/	200	301	41672	1096	405...
3	GET	https://ssl.google-analytics.com:443/__utm...	200	200	556	556	0
4	GET	https://paapi.siteconfidence.co.uk:443/pa/1...	101	101	193	193	0
5	GET	https://metrics.responsetap.com:443/track/...	200	200	588	237	351
6	GET	https://beacon-rumlive.rum.nccgroup-webp...	204	204	740	740	0
7	GET	https://metrics.responsetap.com:443/track/...	200	200	189	189	0
8	GET	https://metrics.responsetap.com:443/track/...	200	200	241	241	0
9	GET	https://metrics.responsetap.com:443/track/...	200	200	241	241	0
10	GET	https://metrics.responsetap.com:443/track/...	200	200	241	241	0
11	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
12	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
13	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
14	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
15	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
16	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
17	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0
18	GET	https://metrics.responsetap.com:443/track/...	200	200	242	242	0

Base Replacements

Add Edit Remove

Enabled	Type	Match	Replace	Which	Comme...	Regex ...

Replacements

Add Edit Remove

Enabled	Type	Match	Replace	Which	Comme...	Regex ...
☑	Reques...	trust	com	Replace...		☐

Conditions

Add Edit Remove

Enabled	Boolean Op...	Match Type	Match Relati...	Match Con...
☑		Sent From ...	Burp	
☐	Or	Request	Contains Pa...	
☐	Or	HTTP Method	Does Not M...	(GET|POST)

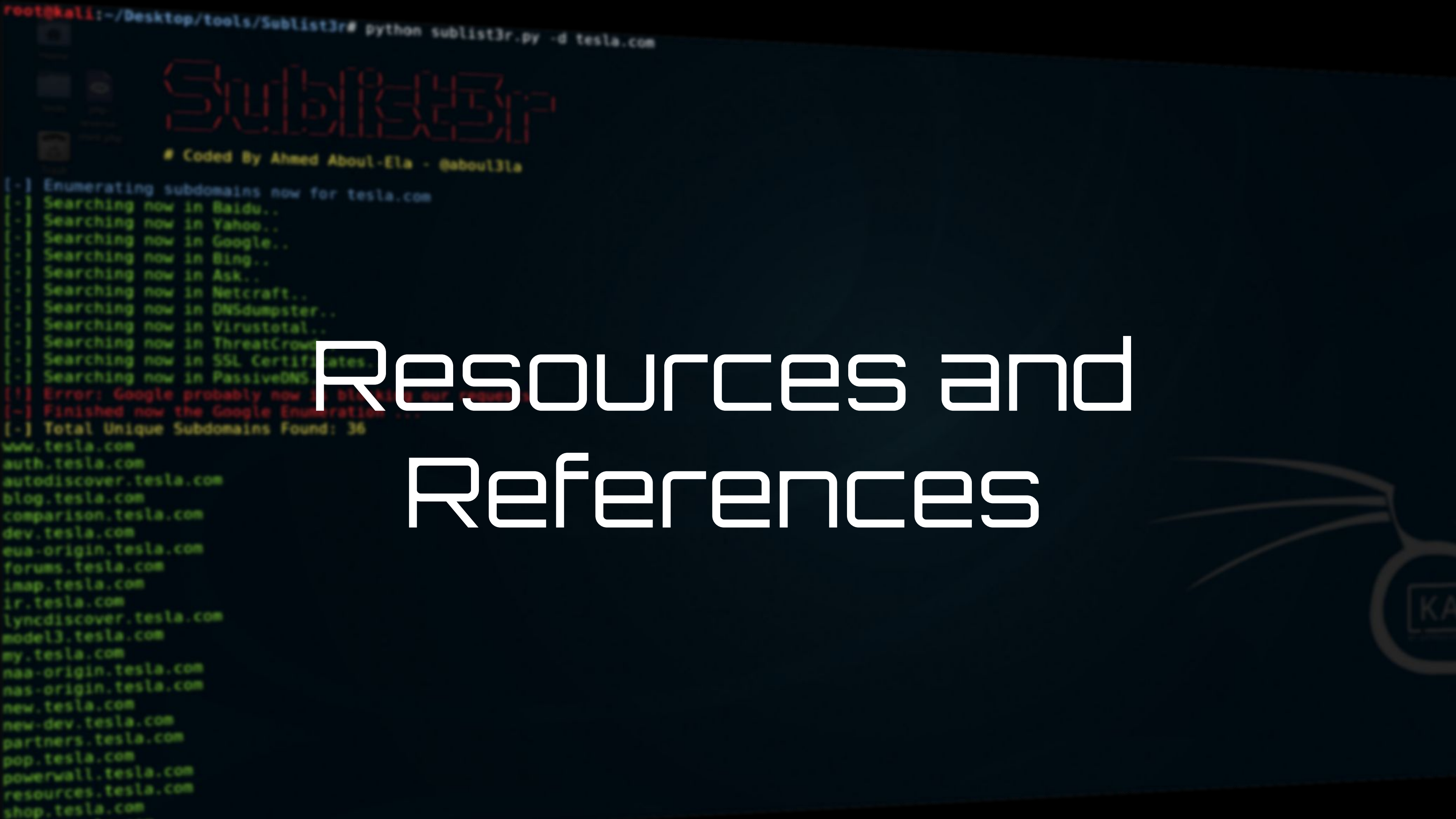
Request

```
GET
/api/Beacon?dns=1516300920331&rt.start=navigation&ds=1516300920330&rt.bstart=15163009
 HTTP/1.1
GET
/api/Beacon?dns=1516300920331&rt.start=navigation&ds=1516300920330&rt.bstart=15163009
HTTP/1.1
Host: beacon-rumlive.rum.nccgroup-webperf.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Geck
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.nccgroup.trust/us/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: SCOSID=7e53ea67-98d2-46b8-867b-93c2df7a0489; SCOGID=3a60c0b8-31c7-492d-ac9
```

Response

```
HTTP/1.1 204 No Content
Access-Control-Allow-Headers: Origin, X-Requested-With, X-Customer-For, Content-Type,
Accept
Access-Control-Allow-Methods: GET, PUT, POST, DELETE, HEAD,OPTIONS
Access-Control-Allow-Origin: *
Cache-Control: no-cache
Date: Thu, 18 Jan 2018 18:42:04 GMT
Date: Thu, 18 Jan 2018 18:42:05 GMT
Expires: -1
Pragma: no-cache
Server: Microsoft-IIS/7.5
Set-Cookie: SCOSID=7e53ea67-98d2-46b8-867b-93c2df7a0489; domain=beacon-rumlive.
rum.nccgroup-webperf.com; path=/; httponly
Set-Cookie: SCOGID=3a60c0b8-31c7-492d-ac96-9aa89f517846; max-age=31536000;
domain=beacon-rumlive.rum.nccgroup-webperf.com; path=/; httponly
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Connection: Close
```

Resources and References



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

References

AutoRepeater	● https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/january/autorepeater-automated-http-request-repeating-with-burp-suite/ ● https://github.com/nccgroup/AutoRepeater ● https://www.youtube.com/watch?v=IYFLp_4ccrw
AuthMatrix	● https://www.youtube.com/watch?v=x2uTYy72ebg ● https://www.youtube.com/watch?v=pMXTmXUsEL8
AuthZ	● https://github.com/wuntee/BurpAuthzPlugin