



# OWASP

Open Web Application  
Security Project

## Amazon Cloud Security Testing 101

Federico De Meo, Security Consultant,  
MindedSecurity

OWASP Italy Day  
Milano, 14<sup>th</sup> March 2019

# TOC

- Once upon a time ...
- What are clouds made of?
- Amazon AWS
  - S3
  - EC2
  - CloudFront
  - Cognito



# Why Amazon??

We encounter it a lot ...  
everywhere!

(not sponsored in any way, shape or form)

[https://www.owasp.org/index.php/OWASP\\_Cloud\\_Testing\\_Guide](https://www.owasp.org/index.php/OWASP_Cloud_Testing_Guide)



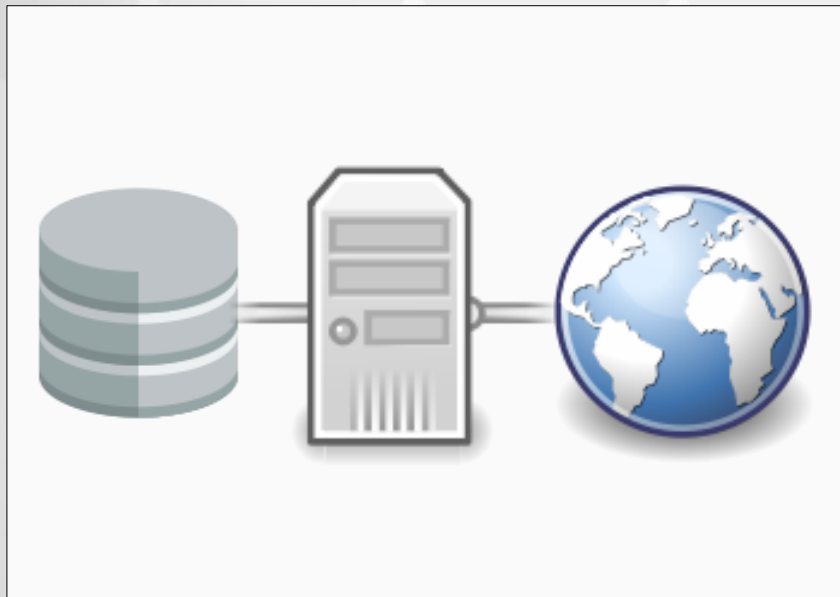
**OWASP**  
Open Web Application  
Security Project

# One upon a time ...

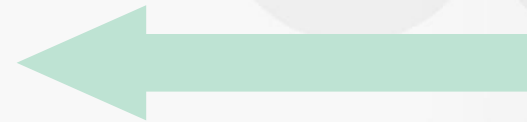
CONNECT.

LEARN.

GROW.



Users



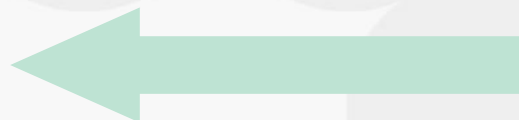
**OWASP**  
Open Web Application  
Security Project

# ... while today!

CONNECT.

LEARN.

GROW.



Users



Your stuff is ... somewhere in there!



Google Cloud Platform



**OWASP**  
Open Web Application  
Security Project

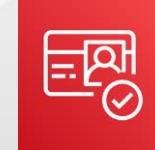
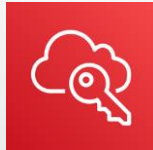
# What are clouds made of?



A place where  
you can **do** stuff



A place where  
you can **store** stuff



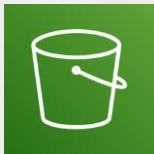
**OWASP**  
Open Web Application  
Security Project

# Amazon AWS

CONNECT.

LEARN.

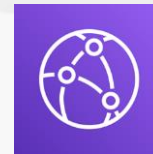
GROW.



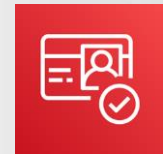
Simple Storage  
Service (S3)



Elastic Compute  
Cloud (EC2)



CloudFront

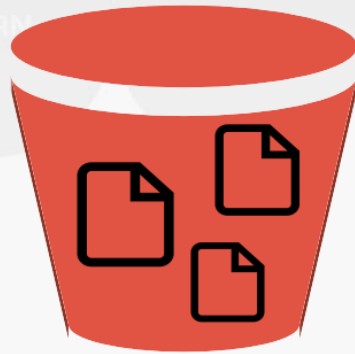


Cognito



**OWASP**  
Open Web Application  
Security Project

# Simple Storage Service (S3)




Is a container of stuff ...possibly sensitive stuff!!





# Simple Storage Service (S3)




SECURITY THROUGH...WHAT EXACTLY? —

## Defense contractor data in Amazon cloud [Updated]

Booz Allen Hamilton engineer posted gist

SEAN GALLAGHER - 5/31/2017, 10:00 PM




TECH REVIEWS SCIENCE ENTERTAINMENT VIDEO FEATURES MORE

MOBILE TECH VERIZON

## Verizon partner data breach exposes millions of customer records

Accessed through an unprotected Amazon S3 storage server



Product Customers Partners Resources Company

Request a Demo

## Skyhigh Discovers GhostWriter: MITM Exposure In Cloud Storage Services

# S3 Security Testing



Acquire target...



...FIRE!!!



**OWASP**  
Open Web Application  
Security Project

# S3 Buckets Identification

**HTML inspection:** find buckets directly in HTML

```
<div class="col-md-3 col-sm-4 col-xs-8">
<div class="logo fadeInLeft wow">

</div>
</div>
<!-- logo -->
```

**Brute-force\educated guessing:** your company name is aegea?

Your bucket might be called **aegea[-something]**

**Google Dork:** let Google do it for you.  
Technique that uses Google Search and  
other Google applications to find security

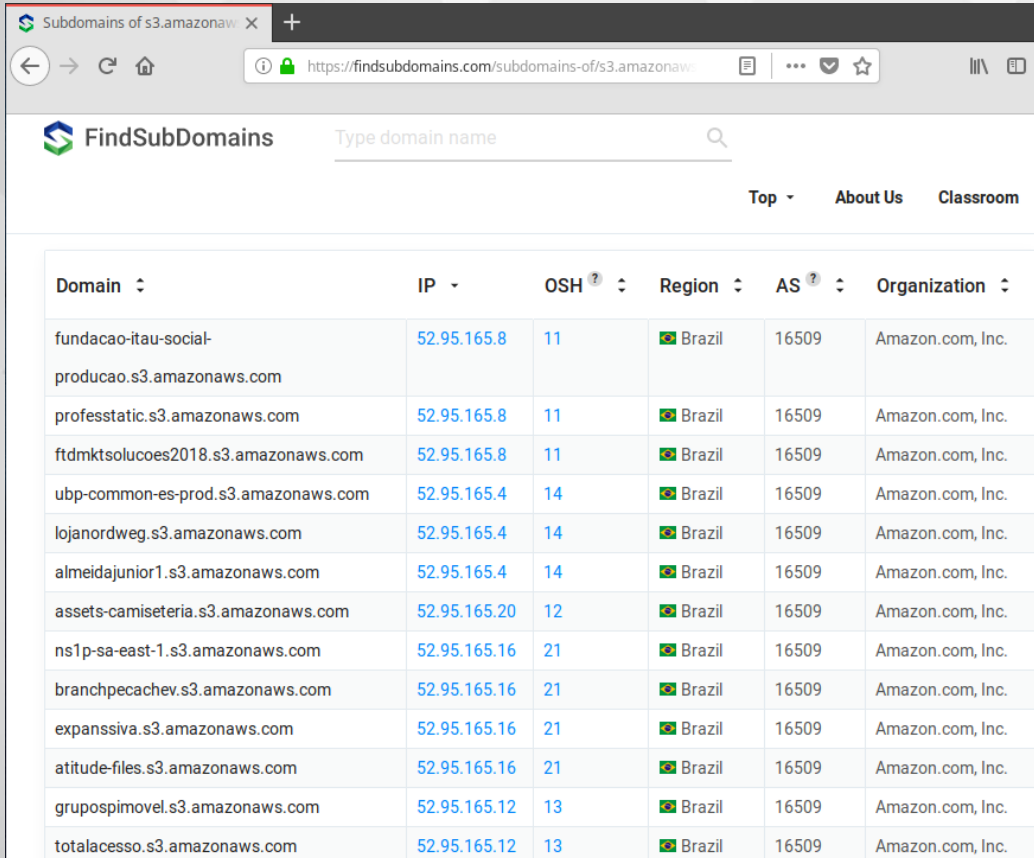
Inurl: s3.amazonaws.com/legacy/  
Inurl: s3.amazonaws.com/uploads/  
Inurl: s3.amazonaws.com/backup/  
Inurl: s3.amazonaws.com/mp3/



**OWASP**  
Open Web Application  
Security Project

# S3 Buckets Identification

**DNS Caching:** let others do it for you



The screenshot shows a web browser window with the URL <https://findsubdomains.com/subdomains-of/s3.amazonaws.com>. The page features the FindSubDomains logo and a search bar. Below the search bar, there are links for 'Top', 'About Us', and 'Classroom'. The main content is a table listing subdomains with columns for Domain, IP, OSH, Region, AS, and Organization.

Domain	IP	OSH	Region	AS	Organization
fundacao-ita-social-producao.s3.amazonaws.com	52.95.165.8	11	Brazil	16509	Amazon.com, Inc.
professtatic.s3.amazonaws.com	52.95.165.8	11	Brazil	16509	Amazon.com, Inc.
ftdmktsolucoes2018.s3.amazonaws.com	52.95.165.8	11	Brazil	16509	Amazon.com, Inc.
ubp-common-es-prod.s3.amazonaws.com	52.95.165.4	14	Brazil	16509	Amazon.com, Inc.
lojanordweg.s3.amazonaws.com	52.95.165.4	14	Brazil	16509	Amazon.com, Inc.
almeidajunior1.s3.amazonaws.com	52.95.165.4	14	Brazil	16509	Amazon.com, Inc.
assets-camiseteria.s3.amazonaws.com	52.95.165.20	12	Brazil	16509	Amazon.com, Inc.
ns1p-sa-east-1.s3.amazonaws.com	52.95.165.16	21	Brazil	16509	Amazon.com, Inc.
branchpecachev.s3.amazonaws.com	52.95.165.16	21	Brazil	16509	Amazon.com, Inc.
expanssiva.s3.amazonaws.com	52.95.165.16	21	Brazil	16509	Amazon.com, Inc.
atitude-files.s3.amazonaws.com	52.95.165.16	21	Brazil	16509	Amazon.com, Inc.
grupospimovel.s3.amazonaws.com	52.95.165.12	13	Brazil	16509	Amazon.com, Inc.
totalacesso.s3.amazonaws.com	52.95.165.12	13	Brazil	16509	Amazon.com, Inc.

Services maintaining a cache of Domain ↔ IP address

You can perform any type of search and hopefully get the bucket you're looking for



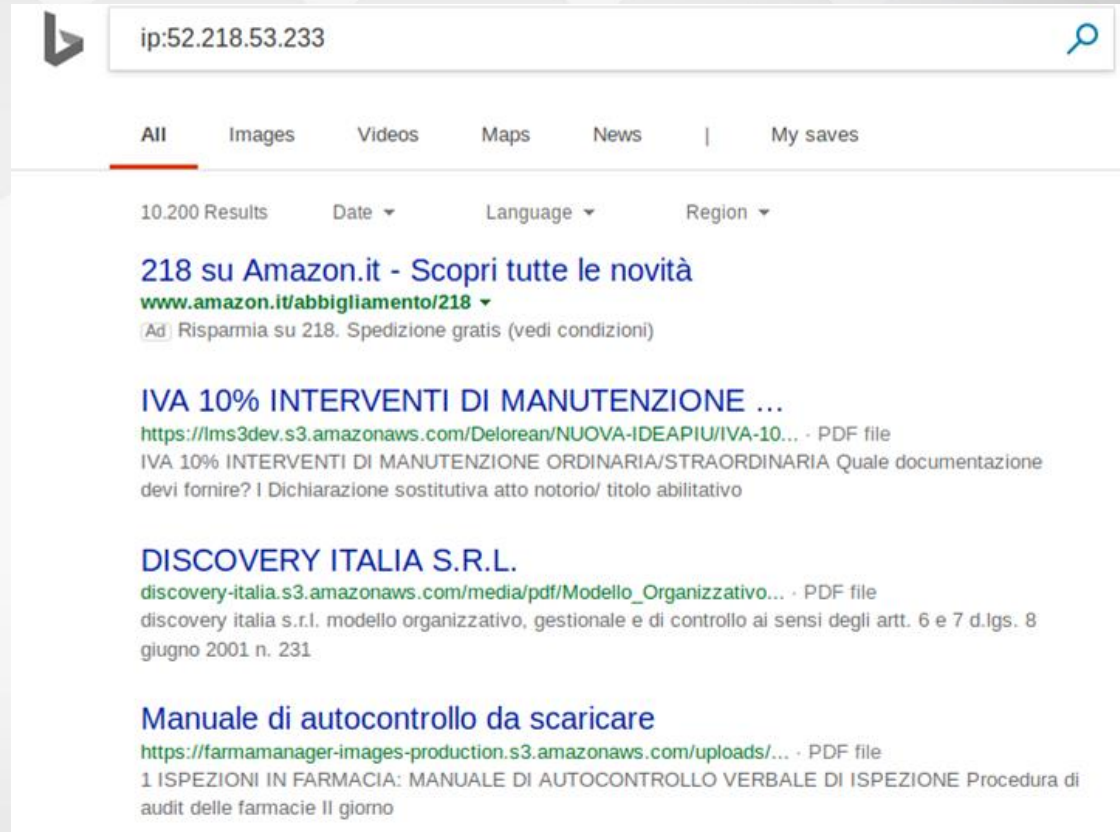
**OWASP**  
Open Web Application  
Security Project

# S3 Buckets Identification

**Bing reverse IP:** who said Microsoft is useless?

... let Bing do it for you

Search for an S3 ip  
and you'll get the bucket  
associated if they appear  
somewhere



ip:52.218.53.233

All Images Videos Maps News | My saves

10.200 Results Date ▼ Language ▼ Region ▼

**218 su Amazon.it - Scopri tutte le novità**  
[www.amazon.it/abbigliamento/218](http://www.amazon.it/abbigliamento/218) ▼  
Ad Risparmia su 218. Spedizione gratis (vedi condizioni)

**IVA 10% INTERVENTI DI MANUTENZIONE ...**  
<https://lms3dev.s3.amazonaws.com/Delorean/NUOVA-IDEAPIUI/IVA-10...> - PDF file  
IVA 10% INTERVENTI DI MANUTENZIONE ORDINARIA/STRAORDINARIA Quale documentazione devi fornire? I Dichiarazione sostitutiva atto notorio/ titolo abilitativo

**DISCOVERY ITALIA S.R.L.**  
[discovery-italia.s3.amazonaws.com/media/pdf/Modello\\_Organizzativo...](https://discovery-italia.s3.amazonaws.com/media/pdf/Modello_Organizzativo...) - PDF file  
discovery italia s.r.l. modello organizzativo, gestionale e di controllo ai sensi degli artt. 6 e 7 d.lgs. 8 giugno 2001 n. 231

**Manuale di autocontrollo da scaricare**  
<https://farmamanager-images-production.s3.amazonaws.com/uploads/...> - PDF file  
1 ISPEZIONI IN FARMACIA: MANUALE DI AUTOCONTROLLO VERBALE DI ISPEZIONE Procedura di audit delle farmacie Il giorno



**OWASP**  
Open Web Application  
Security Project

# S3 Permissions Testing

## READ

```
aws s3 ls s3://[bucketname] --no-sign-request
```

## WRITE

```
aws s3 cp localfile s3://[bucketname]/test-upload.txt --no-sign-request
```

## READ\_ACP

```
aws s3api get-bucket-acl --bucket [bucketname] --no-sign
```

## WRITE\_ACP

```
aws s3api put-bucket-acl --bucket [bucketname] [ACLPERMISSIONS] --no-sign-request
```

<https://blog.mindedsecurity.com/2018/09/a-practical-guide-to-testing-security.html>

# Elastic Compute Cloud (EC2)

... in other words, Virtual Machines on Amazon.

## Interesting features:

1) It can be combined with other AWS Services such as S3 to save snapshots.



AWS EC2



EBS  
Snapshot  
in AWS S3

2) There's a specific end-point <http://169.254.169.254> that can be queried to get juicy info about the EC2 instance





# Publicly accessible EC2 snapshots

This can be real fun ... for everyone.

People take snapshots of their EC2 instance and leave them publicly accessible.

CONNECT. LEARN. GROW.

Public Snapshots ▾					
search : backup × Add filter ?					
<input type="checkbox"/>	Nan ▾	Snapshot ID ▾	Size ▾	Description ▴	Status
<input type="checkbox"/>		snap-0fb8fee1799b...	200 GiB	ak backup	● completed
<input type="checkbox"/>		snap-0e793674b08...	30 GiB	backup	● completed
<input type="checkbox"/>		snap-041c06c0c36...	8 GiB	backup	● completed
<input type="checkbox"/>		snap-0aea9ed9afa6...	100 GiB	Backup	● completed
<input type="checkbox"/>		snap-0ee8c06d984...	100 GiB	echo backup	● completed
<input type="checkbox"/>		snap-0fae9ca3c7ac...	30 GiB	kharon-s3-transition-backup	● completed
<input type="checkbox"/>		snap-07072db1e2e...	500 GiB	TestTags Mon Dec 12 15:21:25 CST 20...	● completed

All you need is an EC2 instance and you can mount any EC2 snapshot in it.



# Metadata leakage

Having access to <http://169.254.169.254> via the EC2 instance allows to have access to many juicy info.

<a href="http://169.254.169.254/latest/meta-data/ami-id">http://169.254.169.254/latest/meta-data/ami-id</a>	The AMI ID used to launch the instance.
<a href="http://169.254.169.254/latest/meta-data/iam/security-credentials/">http://169.254.169.254/latest/meta-data/iam/security-credentials/</a>	If there is an IAM role associated it returns its name (which can be used in the next handler).
<a href="http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name">http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name</a>	If there is an IAM role associated with the instance, role-name is the name of the role, and role-name contains the temporary security credentials associated with the role (for more information, see Retrieving Security Credentials from Instance Metadata). Otherwise, not present.
<a href="http://169.254.169.254/latest/user-data">http://169.254.169.254/latest/user-data</a>	Returns a user-defined script which is run every time a new EC2 instance is launched for the first time.

# Nice ... but how?

- Proxy feature
- Server-Side Request Forgery
- DNS Rebinding
- ...any other way to make a request through an EC2

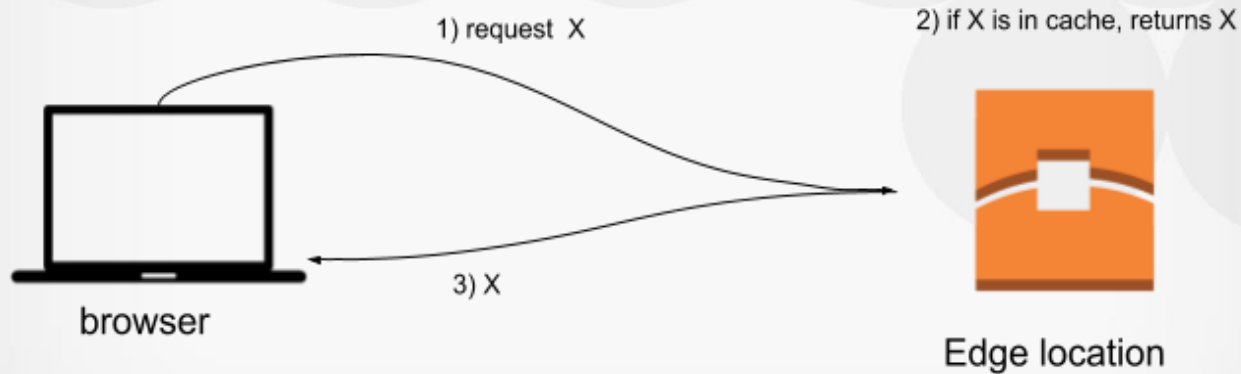
[https://blog.mindedsecurity.com/2018/09/a-practical-guide-to-testing-security\\_18.html](https://blog.mindedsecurity.com/2018/09/a-practical-guide-to-testing-security_18.html)



**OWASP**  
Open Web Application  
Security Project

# CloudFront

Content Delivery Network (**CDN**) helps deliver things faster.

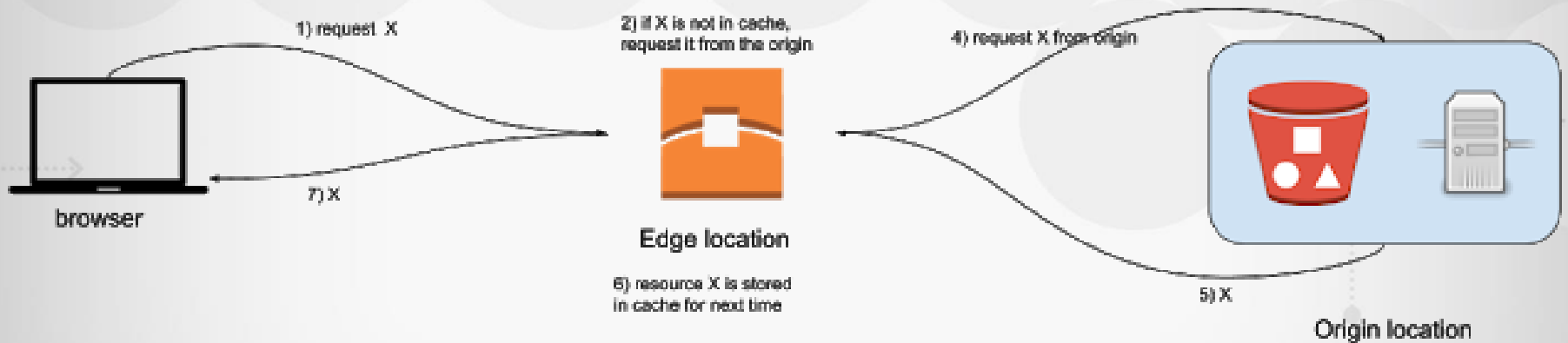


# CloudFront

CONNECT.

LEARN.

GROW.



**OWASP**  
Open Web Application  
Security Project

# Practical Web Cache Poisoning

(by James Kettle)

A CDN needs a way to uniquely identify a request.

Some parts of the HTTP request are used for such unique identification.

If the cache keys change, ask new version, otherwise serve a cached version.

GET /en?cb=1 HTTP/1.1

Host: www.redhat.com

X-Forwarded-Host: canary

HTTP/1.1 200 OK

Cache-Control: public, no-cache

...

<meta property="og:image"

content="https://canary/cms/social.png" />



# Practical Web Cache Poisoning

(by James Kettle)

```
GET /en?cb=1 HTTP/1.1
Host: www.redhat.com
X-Forwarded-Host: a."><script>alert(1)</script>
HTTP/1.1 200 OK
Cache-Control: public, no-cache
...
<meta property="og:image"
content="https://a."><script>alert(1)</script>/cms/social.
png" />
```

X-Forwarded-Host is not a cache key.

If I manage to force CloudFront to save this request, other users will get XSSed.

<https://portswigger.net/blog/practical-web-cache-poisoning>

# Cognito

AWS Cognito provides developers with an authentication, authorization and user management system that can be implemented in web applications.

**identity pools** as they provide access to other AWS services that we might be able to mess with

## ▼ Unauthenticated identities ⓘ

Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials you can enable access for unauthenticated identities. [Learn more about unauthenticated identities.](#)

☒ Enable access to unauthenticated identities



# Cognito

Identity ID: us-east-2:ddeb887a-e235-41a1-be75-2a5f675e0944

Request ID: cb3d99ba-b2b0-11e8-9529-0b4be486f793

SecretKey: wJE/[REDACTED]Kru76jp4i

AccessKey ID: ASI[REDACTED]MAO3

SessionToken AgoGb3JpZ2luELf[REDACTED]wWeDg8CjW9MPerytwF

Buckets:

**mindeds3log**

**mindeds3test01**

Link?? Coming soon...



**OWASP**  
Open Web Application  
Security Project



# Conclusione





*That's all Folks!*