Web Application & Cloud Computing
What are the new threats?

David Calligaris
OWASP Italy Day
Cagliari, 19th October 2018
$: whoami

- Geek & Nerd
- Director Security Testing Automation Huawei Munich (DE)
- Former CTO Emaze S.p.A.
Disclaimer

All the content of these slides represent my personal view not that of my employer.
What is this presentation about?

- How Cloud Computing changes Companies
- How Cloud Computing changes Web Applications
- Web Applications & External Resources (Buckets)
- Buckets Security
What are Clouds?

- Virtual Machines
- Storage
- Application Providers
- Others ...
Companies before Cloud era:
Companies in Cloud era:
Web Applications before Cloud era:
Web Applications in Cloud era:
Loading External Files

- Web application could load images, javascripts, css from external sources
Loading External Files

• In general this puts your application at risk because the security of your web application depends on the security of these external sources
Loading External Files

• We have several examples and write-ups of security issues of Web Applications loading contents from expired domains

Abandoned Domain Takeover as a Web Security Risk

In the modern web it's extremely common to include third party content on web pages. Youtube videos, social media buttons, ads, statistic tools, CDNs for fonts and common javascript files - there are plenty of good and many not so good reasons for this. What is often forgotten is that including other peoples content means giving other people control over your webpage. This is obviously particularly risky if it involves Javascript, as this gives a third party full code execution rights in the context of your webpage.

I recently helped a person whose Wordpress blog had a problem: The layout looked broken. The cause was that the theme used a font from a web host - and that host was down. This was easy to fix. I was able to extract the font file from the Internet Archive and store a copy locally. But it made me thinking: What happens if you include third party content on your webpage and the service from which you're including it disappears?

I put together a simple script that would check webpages for HTML tags with the src attribute. If the src attribute points to an external host it checks if the host name actually can be resolved to an IP address. I ran that check on the Alexa Top 1 Million list. It gave me some interesting results. (This methodology has some limits, as it won't discover indirect src references or includes within Javascript code, but it should be good enough to get a rough picture.)
Loading External Files

- The consequences could have a high impact:
  - Load in-browser JavaScript cryptominer
  - Steal cookies
  - Inject Malicious code (e.g. malware, exploit)
Loading External Files Buckets

- Sometimes we can see a web application loading content from buckets

Loading External Files Buckets

- What are the differences if an application is loading content from a bucket?
- What are buckets?
What are Buckets?

Services served by different cloud providers (e.g. Amazon S3, Google Storage, DigitalOcean Spaces, etc) that offer storage resources.
In recent years buckets misconfiguration issues were on the news for several security incidents.
Identify buckets

Buckets have a particular name format and are easy to identify:

- `bucket-name.s3.amazonaws.com`
- `s3.amazonaws.com/bucket-name`
- `bucket-name.s3-us-west-2.amazonaws.com`
- `s3-us-west-2.amazonaws.com/bucket-name`
- `bucket-name.storage.googleapis.com`
- `storage.googleapis.com/bucket-name`
Identify buckets

Sometimes buckets are behind a CNAME or CDN:

• d1l27wvezozmw4.cloudfront.net
• images.owaspdaycagliari2018.it
Identify buckets

There are several techniques to identify buckets:

- CNAME
- Server Header
- Default Page
- Error Message
How to identify buckets?

- DNS CNAME

```bash
sh-3.2$ nslookup download.intel.com
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
download.intel.com.s3-us-west-2.amazonaws.com canonical name = s3-us-west-2-r-w.amazonaws.com.
Name: s3-us-west-2-r-w.amazonaws.com
Address: 52.218.201.217
```
How to identify buckets?

- Server Headers (1/2)

HTTP/1.1 403 Forbidden
x-amz-bucket-region: us-east-1
x-amz-request-id: 8F5D2E041612C5AA
x-amz-id-2: 6hAAqc4axNET/TAXh0Taoeo27RV0GpsADNk5K94Q4+NA2fpgjchY5T5Q8jmZEH9SDsc6R0cl44=
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Fri, 12 Oct 2018 14:39:42 GMT
Server: AmazonS3
How to identify buckets?

- Server Headers (2/2)
How to identify buckets?

- “Index” default page

```xml
  <Name>owaspdaytest2018</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>test1.txt</Key>
      <LastModified>2018-10-12T12:06:37.000Z</LastModified>
      <ETag>d41d8cd98f00b204e9800998eccf427e</ETag>
      <Size>0</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
  
  <Contents>
    <Key>test2.txt</Key>
      <LastModified>2018-10-12T12:06:36.000Z</LastModified>
      <ETag>d41d8cd98f00b204e9800998eccf427e</ETag>
      <Size>0</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
  
  <Contents>
    <Key>test3.txt</Key>
      <LastModified>2018-10-12T12:06:35.000Z</LastModified>
      <ETag>d41d8cd98f00b204e9800998eccf427e</ETag>
      <Size>0</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
  
  <Contents>
    <Key>test4.txt</Key>
      <LastModified>2018-10-12T12:06:35.000Z</LastModified>
      <ETag>d41d8cd98f00b204e9800998eccf427e</ETag>
      <Size>0</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
</ListBucketResult>
```
How to identify buckets?

Via “Error Messages”

404 Not Found

- Code: NoSuchKey
- Message: The specified key does not exist.
- Key: index.html
- RequestId: B3722D678AE7E5BF
- HostId: 6Bo0HI55fuQct93GUe1ZLXwkxssLLILSKlpkdhMUhFOqGSQK7aBiK/F8c01qSK1n3YL3Q4UxmQ4=

404 Not Found

- Code: NoSuchWebsiteConfiguration
- Message: The specified bucket does not have a website configuration
How to identify buckets?

- Via 404 “NoSuchBucket” Error Message

```xml
<Text>
<Code>NoSuchBucket</Code>
<Message>The specified bucket does not exist</Message>
<BucketName>test1111111111.x</BucketName>
<RequestId>521DE2B76A2B0E3D</RequestId>
</Text>

<HostId>
ChboJZ6acvwVDocxnMK7fLKpwnvU9rtxmN61wemBHA/rx1dDkU84Nzip3wutnIyRs2ObIwGnbs0=
</HostId>
</Text>
```

NOTE: This can enable a **SubDomain Takeover Vulnerability**
Special Note: Subdomain TakeOver

• The first article regarding this vulnerability is from Franz Rosen from 2014

https://labs.detectify.com/tag/hostile-subdomain-takeover/
Special Note: Subdomain TakeOver

- Companies decide to use a bucket for storing website images:
  - images-owasp.s3.amazonaws.com
Special Note: Subdomain TakeOver

- The company decides to associate this name with a company DNS entry:

  images-owasp.example.com ➔ CNAME ➔ images-owasp.s3.amazonaws.com
Special Note: Subdomain TakeOver

- After some time the company decides to use a different cloud provider for hosting the images and deletes the bucket ...
Special Note: Subdomain TakeOver

• … but they don’t delete the DNS CNAME entry

images-owasp.example.com

CNAME

images-owasp.s3.amazonaws.com
Special Note: Subdomain TakeOver

• Anyone now can create a bucket with the original name and take control of it

images-owasp.example.com

CNAME

images-owasp.s3.amazonaws.com
Special Note: Subdomain TakeOver

• What are the consequences of the SubDomain TakeOver?
  • Phishing Attacks
  • In some conditions Steal Cookies with scope *.example.com
  • In some conditions bypass CORS/CSP Policy
Special Note: Subdomain TakeOver

• Additional Resources:
  – https://github.com/EdOverflow/can-i-take-over-xyz
  – https://0xpatrik.com/subdomain-takeover-basics/
Special Note: Subdomain TakeOver

- Who is to blame?
  - SysAdmins?
  - Cloud Service Providers?
Special Note: Subdomain TakeOver

CVE and Cloud Services, Part 1: The Exclusion of Cloud Service Vulnerabilities

By Kurt Seifried, Director of IT, Cloud Security Alliance and Victor Chin, Research Analyst, Cloud Security Alliance

The vulnerability management process has traditionally been supported by a finely balanced ecosystem of enterprises, and vendors. At the crux of this ecosystem is the Common Vulnerabilities and Exposures (CVE) system. In recent times, these criteria have become more and more common.

This is the first in a series of blog posts that will explore the challenges and opportunities in cloud services.

https://blog.cloudsecurityalliance.org/2018/08/13/cve-cloud-services-part-1/
Testing Buckets Security

- Buckets can be misconfigured in different ways:
  - READ Access
  - WRITE Access
  - Readable ACL
  - Writable ACL
  - ...

Testing Buckets Security

• Buckets can have different types of access:
  – Anonymous
  – Authenticated User (*)
  – Owner
Testing Buckets Security

• Checking for READ Access:

Amazon
$ aws s3 ls s3://bucket-name

Google
$ gsutil ls gs://bucket-name
Testing Buckets Security

• READ Access:
  • Backups (.tar.gz, .zip)
  • SQL Databases (.sql)
  • Source Code (.php, .aspx, .rb)
Testing Buckets Security

• Checking for WRITE Access:

Amazon
$ aws cp TestUpload.txt s3://bucket-name

Google
$ gsutil cp TestUpload.txt gs://bucket-name

NOTE: remember to delete the file!!!
Testing Buckets Security

• WRITE Access:
  • Overwrite files (.js, css, jpg, html)
  • Create phishing pages (.html)
  • Overwrite executables (.exe, .sh)
  • Malware drop zone
  • Warez Hosting
Testing Buckets Security

• Checking ACL READ ACCESS

Amazon

$ aws s3api get-bucket-acl --bucket bucket bucket-name
Testing Buckets Security
Testing Buckets Security

• Checking ACL WRITE ACCESS

Amazon

$ aws s3api put-bucket-acl --bucket bucket-name NEW_ACL
Testing Buckets Security

```json
{
    "Permission": "FULL_CONTROL",
    "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
    },
    "Permission": "WRITE_ACP"
}
```
Testing Buckets Security

• The topic is not over; in this presentation we did not cover some aspects like:
  – Bucket Name Identification
  – Bucket Policies
  – Pre-Signed URLs
Bucket Security

Bad Packets Report @bad_packets · 7 Nov 2017
ICYMI: This was caused by an open @awscloud bucket. After someone found that, installing #Coinhive was a breeze on @Politifact's website!

Bad Packets Report @bad_packets · Mar 2
#Coinhive was removed from @Farmacity's website around 2:20 PM UTC time today. The compromised AWS S3 bucket now returns a 403 Forbidden error.

The CyberWire @thecyberwire · Feb 28
On Podcast: In today’s podcast, we hear that #CoinHive was installed via a misconfigured #AWSS3 bucket. #cybersecurity #infosec bit.ly/cwPod02271
Bucket Security

If you find POC.txt in your S3 bucket you need to secure it asap!

11:48 AM - 5 Dec 2017

Hello from https://www.twitter.com/random_robbie - this is a proof of concept to check if your S3 bucket has incorrect permissions.

Please secure your s3 bucket before a bad guy finds it!!

DM's are open if you wish to chat.

https://www.openbugbounty.org/researchers/Random_Robbie/ (little overview of me)
Conclusions

• Nothing New, just a new contest:
  – Writable FTP Server, Writable NFS Share, Writable Buckets

• Need of Security Automation:
  – Traditional security scanners focus on old / classic perimeter
  – We need new security scanners to check cloud deployment
Thanks!

Feedback: david.calligaris@gmail.com