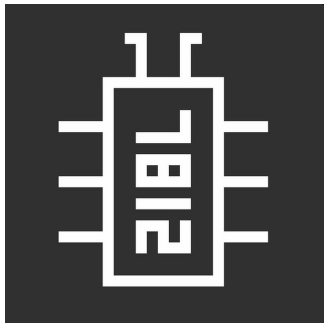
Severe Consequences of a Misconfiguration

Leading web security solution

About Me

- Security researcher at Acunetix
- Web security enthusiast / pentester
  https://github.com/GrrrDog/
  https://twitter.com/antyurin
- Co-organizer of Defcon Russia 7812
  https://t.me/DCG7812



“Signed” Cookie

A cookie with a signature (MAC)
Data tampering with known secret

“Signed” Cookie

A cookie with a signature (MAC)

sess=eyJ0ZXN0IjoiMTIzIn0.XbLGjw.y2xE2iy_LsK816oy4Scm8O9Ve4A

eyJ0ZXN0IjoiMTIzIn0.XbLGjw - value (data.timestamp)
y2xE2iy_LsK816oy4Scm8O9Ve4A - MAC/signature

eyJ0ZXN0IjoiMTIzIn0 - Base64({"test":"123"})
y2xE2iy_LsK816oy4Scm8O9Ve4A - Base64(HMAC-SHA1(value))

MAC

HMAC(secret, value)

- Hash function (MD5, SHA1, etc)

- No secret? No valid signature

- Data tampering protection

Why?

- The cookie is on the client side

- Store session data in the cookie

- Load balancing

- etc.

Frameworks/libraries

- Flask
- Django
- Web2py
- RoR
- ...
- Express
- Shiro
- Mojolicious
- JWT *
- ...

Variations (URL decoded)

eyJ0ZXN0IjoiMTIzIn0.XbLGjw.y2xE2iy_LsK816oy4Scm8O9Ve4A

.eJyrVipJLS5RslJKHDigpAN2hNEAu6IWACPhY5E.XbQZOw.4zw650xetB13gaCDzvAD6JULMGA

s:JH9Gp4UKbN3JOCPQG0AI1H8sFw4VCu0l.llxo+WcGgg4tSX2Ni8kozj6Ni5ledF2AKyo2d995+3M

c4e1213a0f6fdd6281718ee0211aab40:2UPUY95IyOA2jY-3N0_FLQtCTZPDlaBEqszVb5jHTcmqqWYlEpfvMD5NU8gfm5nnPcWyVZZRynFCilwiokXIzzYC1eV4Vub2ihHvZYWSsQPvBuNrGtUdOjwrLQ-3QFM7ZsnHL6FFFeNwY28U36RL1RerNftbLg13c5SzytUp7mK6ojgZvaBjHPYllvkOHITjK0RPqaspOPQ_2XIZvb9XCs-8HgZIG0ltdUBeAdmzR6bj23yPdKy_lZCz5PO4mh-KiyYeKqPosF7qJbsKQlgIfvrgD1lcGXgq5i3yczQ9QvGwyjwiV0JwOji9mJ4F6BRq

Consequences

Authentication bypass

PeopleSoft - ERP

- PS_TOKEN cookie – SSO
- The cookie contains user name
- TokenChpoken attack https://bit.ly/2NiUjwX
- Node password => PS Admin
  - UserID
  - Language Code
  - Date and Time Issued
  - Issuing System – Node name
  - Signature = SHA1_Hash (UserID + Lang + Date Time issued + Issuing System + Node Password)

Consequences

Deserialization

- Web frameworks serialize objects to values in cookies

web2py (CVE-2016-3957)

- Uses Python's Pickle
- RCE as a feature

- https://devco.re/blog/2017/01/03/web2py-unserialize-code-execution-CVE-2016-3957/

Consequences

Deserialization

- Web frameworks serialize objects to values in cookies

Apache Shiro (CVE-2016-4437) *

- Uses Java native binary serialization
- RCE using gadgets
- * - encrypted

- https://www.seebug.org/vuldb/ssvid-92180

Consequences

Nothing?

- Express express-session
  - “s:base64(value):base64(hmac-sha256)”
  - value – random id
- Detect framework

Secret

Where does it come from?

- Secure random value

- Developer must set it (!!!)
  - No value
  - Hardcoded value
  - Insecure generation

How to Get the Secret?

Bruteforce – HashCat

Hashmode: 150 – HMAC-SHA1
GeForce GTX 1080 Ti – **2410.7 MH/s**

a-zA-Z0-9, length – 8: **24 hours**

- Long values could reduce the speed

https://github.com/siseci/hashcat-benchmark-comparison/

How to Get the Secret?

Documentation/examples

- Hardcoded (default) value

- Insecure generation
  - Secret == filename main file
  - Secret == main package name

- People like copying code

BigQuery and GitHub

Google BigQuery

- NoSQL, SQL, BigData, MapReduce…
- BigQuery engine or Cloud Dataflow engine
- Can process huge amounts of data super fast

- 1 TB/mo for free + 300$

- A bunch of examples:
  https://medium.com/google-cloud/github-on-bigquery-analyze-all-the-code-b3576fd2b150

BigQuery and GitHub

Google BigQuery

- Public dataset of GitHub public repositories
- Over 3M GitHub repositories

- 3*10^9 files
- About 3 TB of data
- Updated weekly

- https://console.cloud.google.com/marketplace/details/github/github-repos

BigQuery and GitHub

bigquery-public-data.github_repos.files

48	crowdtap/clearance	refs/heads/master	spec/rails_root/vendor/plugins/clearance	40960	0ec7299e4a35db3cc31b820318e9629d3691fae1
49	mczepiel/introduction	refs/heads/master	node_modules/montage	57344	601f849e86150f427ebe49bef8317b3fcf4488f2
50	Bilb/vtm	refs/heads/master	vtm-ext-libs	57344	194dac648666d3e6aac3fd8fbee05684718fa156
51	Bilb/vtm	refs/heads/master	appcompat	57344	eead2062deaeda844de58777247f517427459e0d
52	Bilb/vtm	refs/heads/master	jni/jni/libtess2	57344	a43504d78a5695ca07cf3706e34abfdfd5b4343b
53	AEinsam/HabReader	refs/heads/master	AndroidBillingLibrary	57344	3ecc7cad9cb6ca55d0de607e03b717876212178d
54	AEinsam/HabReader	refs/heads/master	ActionBarSherlock	57344	9598f2bb2ceed4a834cd5586a903f270ca4c0ccc
55	AEinsam/HabReader	refs/heads/master	SlidingMenu	57344	ef53ae599e3c470a97161c7d0a97255d0ff18610
56	PaoloW8/android_kernel_nubia_nx505j	refs/heads/cm12.1	arch/microblaze/boot/dts/system.dts	40960	7cb657892f21229d0068d2e7416e91e551264f77
57	snowplow/dev-environment	refs/heads/master	ansible-playbooks	57344	d99126e9aab548cc434e83aa2ef1121a5fec0930
58	benderTheCrime/django-app-flag	refs/heads/master	include/python2.7	40960	3fe034fccc4d0415e58e049aaf9174ec86bdaf89
59	Relearn/closedloopcoast-client	refs/heads/master	node_modules/.bin/json2dsv	40960	a4e6866fe57f697afccb4e7f6282485a8d8cfcac

BigQuery and GitHub

```
SELECT * FROM
    `bigquery-public-data.github_repos.files`
     WHERE ENDS_WITH(path, '.java')
```

- Query settings -> Set a destination table for query results
- Allow large results (no size limit)

BigQuery and GitHub

SQL / legacy SQL

```
SELECT * FROM `bigquery-public-data.github_repos.sample_files`
WHERE ENDS_WITH(path, '.java')
```

```
SELECT * FROM [bigquery-public-data:github_repos.files]
WHERE RIGHT(path, 5) = '.java'
```

BigQuery and GitHub

bigquery-public-data.github_repos.contents

			import java.io.File;
19	6ae35d269efe02a749d22da48337a3e30f1db6ab	1552	package com.vivifram.second.hitalk.bean.parser; import com.avos.avoscloud.AVObject; import com.avos.avoscloud.AVUser; import com.vivifram.second.hitalk.bean.blackboard.BnCommentRemote; import com.vivifram.second.hitalk.bean.blackboard.BnItem; import com.vivifram.second.hitalk.bean.blackboard.BnRemote; import com.vivifram.second.hitalk.bean.blackboard.CommentItem;
20	d355185aca6c8ba968cdbb9ad30b18d7f8c22c0a	627	package com.matt.taskel.tasks; import com.matt.taskel.logging.Level; import com.matt.taskel.util.FileUtil; public class SetupForge extends Task { public SetupForge()

BigQuery and GitHub

```
#legacySQL
SELECT  content.restr,  files.repo_name, files.ref, files.path
FROM (
  SELECT

     REGEXP_EXTRACT(line, r'([\\\s]*\'cookieValidationKey\'\s*=>\s.+)') AS restr

  FROM (

     SELECT  SPLIT(content, '\n') AS line
     FROM    [github_extracts.all_php_contents] )

   HAVING  restr IS NOT NULL ) AS content
JOIN  [github_extracts.all_php_files] AS files
ON content.id = files.id
```

Search in Docker Containers

- Inside the container

docker run -it schmunk42/yii2-app-basic /bin/bash

find . -name *.php -print0 | xargs -0 grep "'cookieValidationKey'"

- No bash/find installed

Search in Docker Containers

- On the host system

```
docker create schmunk42/yii2-app-basic
docker export container_id > yii2.tar
zgrep -a "cookieValidationKey" yii2.tar
```

if we need a filename:

```
tar xaf yii2.tar  --to-command="awk -e '/cookieValidationKey/
    {print ENVIRON[\"TAR_FILENAME\"] \":\", \$0}'"
```

Found Secrets

- Depends on frameworks
- 30-15000
- 15-3000 uniques
- Secret leakage

Why?

```
awk -F ',' '{print $1}' secrets.csv | sort | uniq -c | sort
```

- Frameworks on frameworks
- Templates/”builders”
- Vulnerable apps
- Common dictionary
- “Change this immediately” -> “changed”
- Tests

Results

1. **Yii2**

   500 random sites -> 12 secrets (3 spec)

1. **Flask**

   200 random sites -> 18 secrets (4 spec)

1. TBA

   60 random sites -> 2 secrets (2 spec)

Universal Detector

How many variations?

1) Separators: :, ., --, no sep

1) Sign position: prefix, suffix

1) Format: hex, (urlsafe)base64

1) HMAC: MD5, SHA1, SHA256 (SHA*)

Universal Detector

Approach:

1) Detect sign (regexs + length)

1) Separate value

1) Dictionary attack on the value

Universal Detector

Results on 2k BugBounty sites:

- Detected: 130
- “Unknown” format: 3
- Secrets: 0 ^_^

More

More info later:

- https://github.com/GrrrDog/
- https://twitter.com/antyurin

Thank you

Leading web security solution