

# **WEBSCRAMBLER RELOADED**



**KEEP  
CALM  
AND  
GO BACK  
IN TIME**

# **HACKFEST 2013**

## **COMMENT RENDRE LES « SCANNERS WEB » FOUS**

# HACKFEST 2013

## QUATRE PRINCIPES

- Les sites Web sont prévisibles
- Le protocole HTTP offre une grande surface d'attaque
- Il est facile de différencier deux réponses HTTP
- Le protocole HTTP est stateless

# HACKFEST 2013

## TACTIQUES UTILISÉES

- Ralentir les outils
- Rendre les outils plus facilement détectables
- Rendre les outils plus spécifiques

# HACKFEST 2013

## RÉACTIONS

Enthousiasme & Scepticisme


# JANVIER 2014

## SHAPESECURITY ANNOUNCE LE 'WORLD FIRST' BOT WALL

*“The industry has long needed a botwall — a new tier of your security architecture that blocks attacks from bots, malware, and scripts, which are the source or enabler of nearly all breaches.”*  
- Ted Schlein, Kleiner Perkins Caufield & Byers

# JANVIER 2014

## POLYMORPHISME TEMPS RÉEL

BEFORE		AFTER
<pre>&lt;form action="login_form.php"&gt;   &lt;input id="username" name="username"/&gt;   &lt;input id="password" name="password"/&gt;   &lt;input id="rememberMe" name="rememberMe"/&gt;   &lt;input id="login" name="login"/&gt;   &lt;input type="submit"/&gt; &lt;/form&gt;</pre>		<pre>&lt;form action="d94M2eQgBK"&gt;   &lt;input id="v6DbNQEs4z" name="dtTtA6tsmi"/&gt;   &lt;input id="b5KbBSjCT6" name="rWttCLcv3f"/&gt;   &lt;input id="zQNA3ZBgKz" name="R2bHEe3taV"/&gt;   &lt;input id="rvnFbpxKwN" name="HNnQwnUbtm"/&gt;   &lt;input type="submit"/&gt; &lt;/form&gt;</pre>
Simplified HTML		Simple real-time polymorphism Code is different on each page request

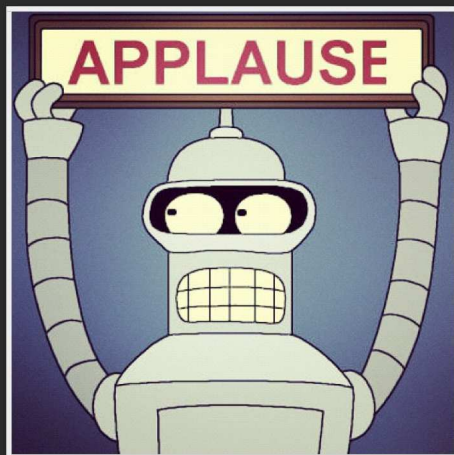
\*Tiré du site Web de ShapeSecurity



# JANVIER 2014

## UN ACCUEIL TRÈS DIFFÉRENT

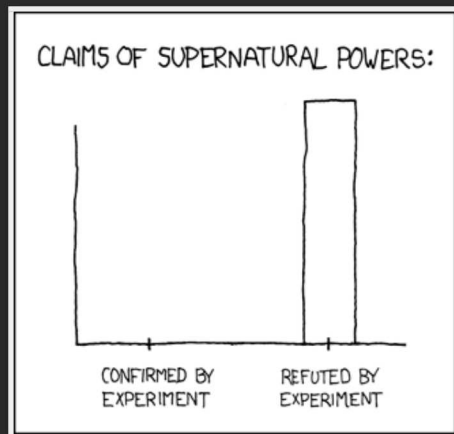
Investisseurs



# JANVIER 2014

## UN ACCUEIL TRÈS DIFFÉRENT

Milieu de la sécurité



# **JANVIER 2014**

## **PRINCIPALES CRITIQUES**

- Les outils vont s'adapter
- Va nuire à la performance

# HACKFEST 2014

## WEB APPLICATION HYPERVISOR (WAH)

*Solution encadrant l'exécution d'application Web  
afin de leur fournir l'environnement d'exécution  
le plus sécuritaire possible.*

LE WAH



# POURQUOI WAH

Comblent le vide laissé par :

- Les serveurs HTTP (Apache, IIS, NGINX, etc.)
- Les Framework (PHP, JEE, .Net, etc.)
- Les développeurs
- Les appareils de sécurité (IDS/IPS, WAF, Bot Wall, etc.)

## WAF

Détecte/bloque les attaques ou les comportements jugés anormaux

- Listes noires
- Listes blanches

≠

## WAH

Empêche de tomber dans un mauvais état d'application

- Frontend = backend

## BOT WALL

Rend l'exécution d'attaques plus complexe

- Polymorphisme temps réel

$\subseteq$

## WAH

Recompile l'application afin d'y intégrer de la sécurité

- Annotation du code
- Modification du code



WAF + BOT WALL + WAH

=



# TYPES POSSIBLES

## HOST BASED

- Serveur HTTP dédié *exclusivement* aux application Web
- Dépendant des langages et FrameWork de développement
- Plus rapide

# TYPES POSSIBLES

## NETWORK BASED

- Analyse, modifie et filtre les communications HTTP entre l'application et l'utilisateur
- Peu convenir à plusieurs technologies de développement
- Moins rapide

# L'OUTIL

- Reverse proxy HTTP (Appliance réseau)
- Aucune signature d'attaques à maintenir
- Choix parmi des politiques de sécurité pré-établies

# CONFIGURATION

General settings

Remote Host:

https://www.example.com/home

Local Host:

https://10.10.0.2/webapp1

Error page:

/error.html

20%

◀ Prev

Next ▶

# CONFIGURATION

Exclusions

?

By default, WAH only works for remote IP addresses. You can change it to be more or less restrictive.

☐ Remote only

☐ All Ip Addresses

☒ Custom set

Please specify the list of IP addresses to exclude

ex: 100.100.2.0-255, 56.24.25.3, 203.35.40.0/24

40%

# CONFIGURATION

Time to live?

Resource time to live is the maximum amount of time a resource can be accessed without WAH indexing it again. Resources are indexed each time they are referred by another accessed resource. Default is 30 days.

*Remark :* Is it not possible to set an absolute time to live

30 days

60%

# CONFIGURATION

Select a policy?

The policy is used to specify the level of protection against attackers. As the level of protection increases, the number of simultaneous requests that can be handled decreases.

**Interactive Web Site**

Level of protection **intermediate**

All content is public with user interactivity. Typically applies to Web Sites with static and dynamic content.

80%



# LES POLITIQUES DE SÉCURITÉ

## UNE COMBINAISON DE

- Surveillance de formulaire
- Surveillance d'URL
- Offuscation d'URL
- Offuscation d'HTML

# LES POLITIQUES DE SÉCURITÉ

SITE INFORMATIONNELS

Niveau de protection

Minimum

# LES POLITIQUES DE SÉCURITÉ

SITE INTERACTIFS

Niveau de protection

Intermédiaire

# LES POLITIQUES DE SÉCURITÉ

SITE AUTHENTIFIÉS

Niveau de protection

Amélioré

# LES POLITIQUES DE SÉCURITÉ

SITE TRANSACTIONNELS

Niveau de protection

Maximum

# SURVEILLANCE DE FORMULAIRES



# ÉTAT DU FORMULAIRE

Le formulaire HTML dicte les valeurs qui doivent être retournées  
au serveur.

# COMPATIBLE HTML5

## HTML5 Introduit de nouveaux type des données

```
<input type="url">  
<input type="email">  
<input type="text" pattern="[0-9A-Za-z]+">  
<input type="number">  
<input type="range" min="0" max="100" step="2">
```



# GESTION INTELLIGENTE DES ERREURS

Côté client et côté serveur.

1. Épure les données
2. Utilise la gestion d'erreur d'HTML 5

# CAS DE FIGURE I

## Épuration de données

```
<select name="cars">
  <option value="volvo">Volvo</option>
  <option value="saab">Saab</option>
  <option value="mercedes" selected>Mercedes</option>
  <option value="audi">Audi</option>
</select>
```

# CAS DE FIGURE I

## Code serveur vulnérable SQLi

```
$query = "SELECT * FROM my_table WHERE model =' " . $_GET["cars"] . "'";  
$result = mysql_query($query)
```

# CAS DE FIGURE I

## Données invalides soumises

```
cars=' UNION (SELECT table_name FROM INFORMATION_SCHEMA.TABLES) #
```

```
cars=bmw
```

# CAS DE FIGURE I

Données reçues par le serveur

```
cars=mercedes
```

# CAS DE FIGURE II

## Gestion d'erreur d'HTML 5

```
<input type="email">
```

# CAS DE FIGURE II

Données invalides soumises

```
victim@victim.com
```

```
<script src="evil.com"></script>
```

# CAS DE FIGURE II

Données non transmises au serveur

Email Address:	victim@victim.com	&lt;script>
		<small>Veuillez saisir une adresse courriel valide.</small>



# RÉSUMÉ

- Simplifie le travail des développeurs
- Mitigue le risque contre beaucoup d'attaques

# SURVEILLANCE D'URL



# ÉTAT D'URL

L'interface graphique dicte les ressources valides d'un site

# CAS DE FIGURE I

## Valeurs permises

```
<a href="/?p=blog">Blog</a>  
<a href="/?p=home">Home</a>  
<a href="/?p=contact">Contact</a>
```

# CAS DE FIGURE I

## Valeurs soumises

```
www.exemple.com/?p=admin  
www.exemple.com/?p="><script>alert(1)</script>  
www.exemple.com/?p=' or ''=  
www.exemple.com/?p=blog&ext=0
```

# CAS DE FIGURE I

URL reçu par le serveur

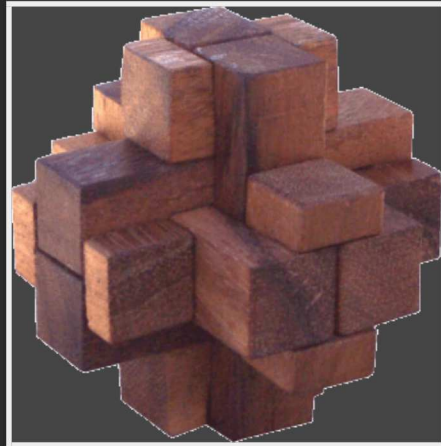
```
www.exemple.com/error.html
```

# CONCRÈTEMENT

Contre l'exploitation des failles techniques dans les URL :

- Injection dans la Querystring - SQLi, XSS, etc.
- Mauvaise configuration - Directory listing, Version non à jour, etc.
- Redirection non validée

# OFFUSCATION D'URL





# POLYMORPHISME D'URL

- Transforme les URL afin :
  - qu'ils ne puissent être devinés
  - qu'ils aient une portée
- Multiples URL pour une même ressource
- Invalide l'URL non « offusqué »

# PORTÉ - SITE

`www.exemple.com/index`

`www.exemple.com/759sv_gLtWOMsY-wB4fALX_8tcFgjRBtNSXSovzPa79whcF-qq7InjWzZiD26c`

# PORTÉ - SITE

- Anti énumération des ressources
- Anti accès direct

# PORTÉ - SESSION

[www.exemple.com/reports/generate?id=3](http://www.exemple.com/reports/generate?id=3)

[www.exemple.com/1YZrQeoZfSc\\_TpTclwt0hNZ4Wne8GJ1LvUpUgbIANv\\_NnPxznmhMIqOh9vvCja](http://www.exemple.com/1YZrQeoZfSc_TpTclwt0hNZ4Wne8GJ1LvUpUgbIANv_NnPxznmhMIqOh9vvCja)

[www.exemple.com/UiNyz8OSn2Z1\\_R6UmPvo7L\\_ikTGy32TBwEI\\_0UC7Wt3PiG\\_lrN33dDHLo3\\_PfA](http://www.exemple.com/UiNyz8OSn2Z1_R6UmPvo7L_ikTGy32TBwEI_0UC7Wt3PiG_lrN33dDHLo3_PfA)

# PORTÉ - SESSION

- Anti rejoute d'une session à l'autre

# PORTÉ - REQUÊTE

## Requête

`www.exemple.com/handleform`

`www.exemple.com/Jag8s5mSfAMOK5Oa1SN5vIgXQY1zdPrOBtfyDbyxW7dRGqKzpInGGvuN2au7UU`

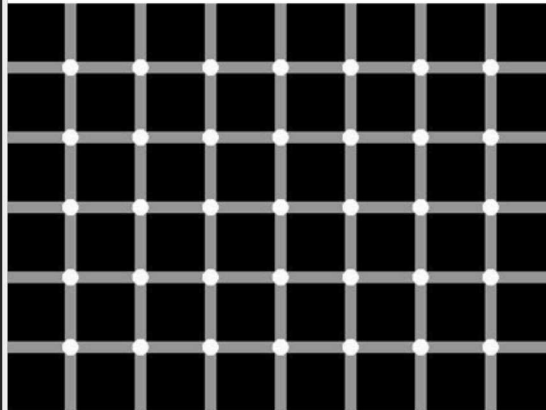
`www.exemple.com/MZYXxJE2VfXv2WAhhjyMZisPV6uS1wIotn4_MwNJEolTb5agc2kW-JBK9h5U2b`

# PORTÉ - REQUÊTE

- Anti rejoute d'une requête à l'autre (Anti CSRF)
- « Anti spidering »

# OFFUSCATION D'HTML

Count all the black dots you can see.



Answer: There are no black dots

If you focus directly on each dot, you'll see that all of them are white.



# TRANSFORME LE HTML

Rend l'analyse des pages Web plus complexe

# LE JAVASCRIPT NOTRE ALLIÉ

```
<script>
  document.write('<div>');
  document.write('<b>');
  document.write('Hello');
  document.write('</b>');
  document.write('World');
  document.write('</div>');
</script>
```

# EXEMPLE

## HTML brute

```
<div>  
  <b>Hello</b> World  
</div>
```

# EXEMPLE

## HTML « offusqué »

```
<html>
<head>
<script src="/wavsep/active/-iUBD3HokAPNrliPWJcjOfMvvUkVJDQAfLiOo1kx4" />
<script>JSON2HTML(document.children[0].children[0], [{"type":"text",
</head>
<body>
<script>
JSON2HTML(document.children[0].children[1], [{"type":"text","data":"\
</script>
</body>
</html>
```

# POURQUOI TRANSFORMER LE HTML?

<https://developers.google.com/webmasters/ajax-crawling/>

# RÉSULTATS



# CONTEXTE

Application vulnérable



# CONTEXTE

Outil de scan





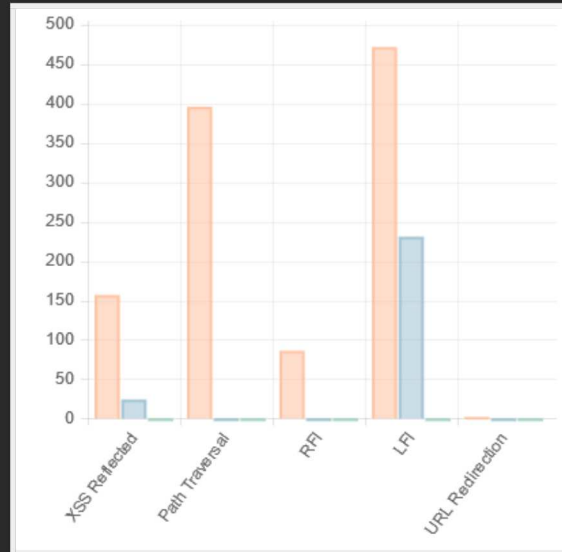
# CONTEXTE

Aucun tri des faux-positifs

# CRAWLING

	URL trouvés
Sans WAH :	1792
Politique minimum :	1792
Politique maximum :	5

# VULNÉRABILITÉS TECHNIQUES



# RÉCAPITULATION



**Fire action**



Sound the alarm



Leave building by nearest available exit



Report to assembly point

Fire assembly point



Do not return to the building until authorised to do so



Do not use the lifts

# WAH

## YASA (YET ANOTHER SECURITY APPLIANCE)

- $WAF \neq BotWall \neq WAH$
- $WAF + BotWall + WAH = \text{Protection accrue}$

# WAH

## LIMITES

- Les applications « manipulateurs de DOM »
- Très grand volume d'utilisation

# WAH

## CIBLE PRINCIPALEMENT

- Les PME
- Les hébergeurs Web

# WAH

## POINTS CLÉS

- Réduit la surface d'attaque
- « Falicite » la tâche aux les développeurs
- Frontend = backend



