

Relever les empreintes d'une application Web



Introduction



Pourquoi ?

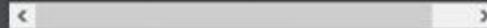
PRINCIPE 1
LES SITES WEB SONT PRÉVISIBLES

Pourquoi ?

LA CONVIVIABILITÉ D'ABORD !

- Structure de répertoire

```
/_layouts/AdminRecycleBin.as  
/_layouts/bpcf.aspx  
/_layouts/create.aspx  
/_layouts/listfeed.aspx  
/_layouts/managefeatures.asp
```



Pourquoi ?

- Chaînes de requêtes

```
/eBayISAPI.dll?ViewFeedback2&userid=halu_games&ftab=AllFeedback&rt=nc&mywo
```

Pourquoi ?

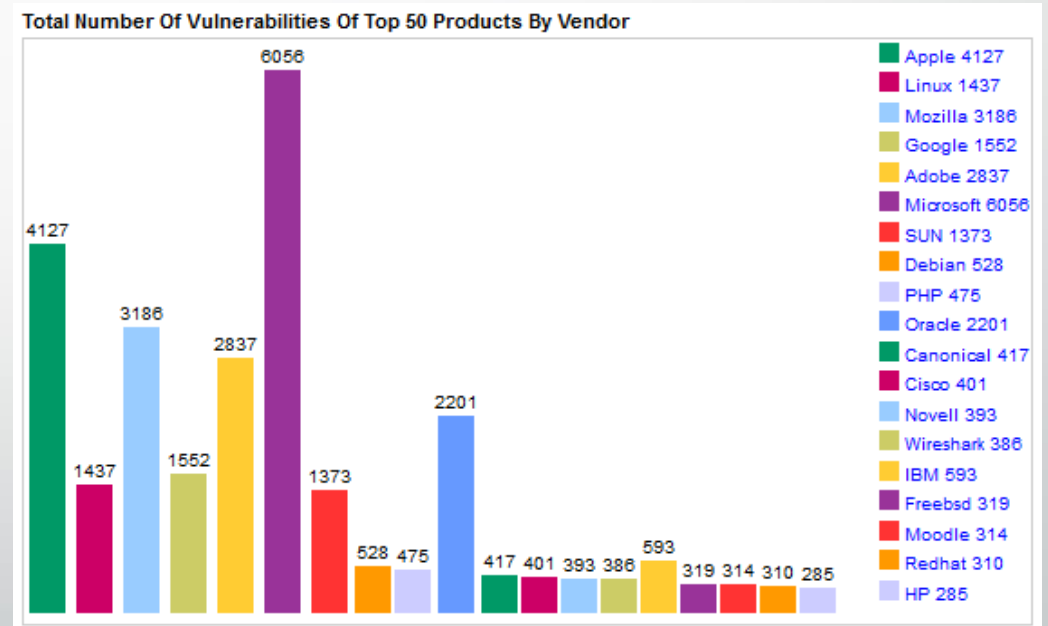
- Formulaires

```
<td>  
<input id="email" name="email" class="inputtext" type="text" tabindex="1" v  
</td>  
<td>  
<input id="pass" name="pass" class="inputtext" type="password" tabindex="2"  
</td>
```

Pourquoi ?

Identifier des vulnérabilités connues

- Il existe nombre incalculable de problématiques documentées;
- Les gens ont tendances à refaire les mêmes erreurs;
- Ne pas recommencer à zéro à chaque fois.



Pourquoi ?

Raffiner ses recherches

- Des contre mesures existent dans plusieurs Framework de développement:
 - CMS versus développement maison
 - PHP versus J2EE versus .NET versus Ruby versus Python versus ...
- « Design pattern » utilisé influence les tests à faire :
 - Forms versus MVC « server » versus MVC « client » (Angular) versus ...

Server Error in '/' Application.

A potentially dangerous Request.Form value was detected from the client (ctl00\$MainContent\$UserName="<qwe></qwe>").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data may attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you may need to modify the web page to explicitly allow it. For more information, see <http://go.microsoft.com/fwlink/?LinkId=212874>.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.Form value was detected from the client (ctl00\$MainContent\$UserName="<qwe></qwe>").

Source Error:

Approche

1. Trouver des « patterns » décrivant une application Web, une technologie, etc;
2. Bâtir une base de connaissances de signatures;
3. Comparer une cible à la base de connaissance.

Plan

- Quelques outils de existants et leurs limites
- À la recherche de signatures « passives »
- À la recherche de signatures « actives »
- Pour une meilleure identification



Quelques outils de existants et leurs limites

Techniques d'identification

Les signatures passives

- Signature basée sur ce qui est divulgué volontairement aux utilisateurs;
- Simule une utilisation « normale » d'une application/site Web;
- Peut être très subtile.

Les signatures actives

- Signature basée sur ce qui est divulgué involontairement aux utilisateurs;
- Requiert l'interaction avec l'application/site Web d'une façon contraire à l'utilisation normale;
- De peu subtile à franc.

Wappalyzer – Signatures








```
"Application Name": {  
  "website": "example.com",  
  "cats":    [ 1 ],  
  "headers": { "X-Powered-By": "Application Name" },  
  "url":     ".+\\.application-name\\.com",  
  "html":    "<link[^>]application-name\\.css",  
  "meta":    { "generator": [ "Application Name", "Alternative Application Name" ] },  
  "script":  "application-name-([0-9.]+)\\.js\\;confidence:50\\;version:\\1",  
  "env":     "ApplicationName",  
  "implies": "PHP\\;confidence:50",  
  "excludes": "Other Application Name"  
}
```

Wappalyzer – Signatures

```
"WordPress": {  
  "cats": [  
    1,  
    11  
  ],  
  "env": "^wp_username$",  
  "html": [  
    "<link rel=[\\\"]stylesheet[\\\"] [^>]+wp-(?:content|includes)",  
    "<link[^>]+s\\d+\\.wp\\.com"  
  ],  
  "icon": "WordPress.svg",  
  "implies": "PHP",  
  "meta": {  
    "generator": "WordPress( [\\d.]+)?\\;version:\\1"  
  },  
  "script": "/wp-includes/",  
  "website": "wordpress.org"  
},
```

Exemple de Wappalyzer











-  **CloudFlare**
CDN
-  **Google Font API**
Font Script
-  **Modernizr**
JavaScript Framework
-  **Nginx**
Web Server
-  **ZURB Foundation**
Web Framework
-  **Google Analytics**
Analytics
-  **jQuery**
JavaScript Framework









Limites de Wappalyzer

- Identification passive;
- Recherche d'expressions régulières à des endroits précis;
- Les signatures à base d'expressions régulières ne fonctionnent pas bien pour tous les cas;
- Ne tient pas compte du contexte;
- Ne permet pas directement le lien avec des vulnérabilités connues;

```
name="tx_stsphinxsearch_search[selectedIndex]">
```


Nikto – Signatures

 db_404_strings	SAP error strings that reply 200 but are really 4xx
 db_content_search	House keeping
 db_dictionary	House keeping
 db_dir_traversal	House keeping
 db_domino	House keeping
 db_drupal	House keeping
 db_embedded	House keeping
 db_favicon	Add Android PAW Server favicon

 db_headers	Add ngx_pagespeed headers
 db_httptoptions	House keeping
 db_multiple_index	Add index.php7
 db_outdated	Update
 db_parked_strings	House keeping
 db_realms	House keeping
 db_server_msgs	Add PAW server for Android server header check
 db_subdomains	Add Issue Tracker related domains

Nikto – Signatures (suite)

Identification passive

- Recherche d'expression régulières dans les réponses:
 - 404
 - URL précis
 - Entête HTTP
- Recherche de HASH de favicon

Identification active

- Accès à des ressources
 - Sous-domaines
 - Chemins d'accès précis
- Accès à des méthodes HTTP;

Limites de Nikto

- Fortement basé sur des expression régulières;
- Notion limitée de contexte;
- Fait peu de lien avec des vulnérabilités connues.

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

WPScan – Signatures passives

```
# @return [ String ] The wp-content directory
def wp_content_dir
  unless @wp_content_dir
    index_body = Browser.get(@uri.to_s).body
    uri_path = @uri.path # Only use the path because domain can be text or an IP

    if index_body[/\Vwp-content\V(?:themes|plugins)\V/i] || default_wp_content_dir_exists?
      @wp_content_dir = 'wp-content'
    else
      domains_excluded = '(?:www\.)?(facebook|twitter)\.com'
      @wp_content_dir = index_body[/(?:href|src)\s*=\s*(?:'|").+#{Regexp.escape(uri_path)}(?:!#{domains_excluded})[^\"]+?)\V(?:themes|plugi
    end
  end

  @wp_content_dir
end
```

WPScan – Signatures passives

```
-<hashes xsi:noNamespaceSchemaLocation="local_vulnerable_files.xsd">
  -<hash sha1="17c372678aafb3bc1a7b37320b5cc1d8af433527">
    <title>XSS in swfupload.swf</title>
    <file>swfupload.swf</file>
    -<reference>
      http://brindi.si/g/blog/vulnerable-swf-bundled-in-wordpress-plugins.html
    </reference>
  </hash>
  -<hash sha1="775dc1089829ef07838406def28a4d8bfef69d66">
    <title>Arbitrary File Upload Vulnerability</title>
    <file>php.php</file>
    -<reference>
      http://packetstormsecurity.com/files/119241/wpvalums-shell.txt
    </reference>
  </hash>
  -<!--
    This one is the same as above, but the postSize verification has been removed
  -->
  -<hash sha1="5e8f0d5a917d2937318a9bafd0529135bd473e70">
    <title>Arbitrary File Upload Vulnerability</title>
    <file>php.php</file>
    -<reference>
      http://packetstormsecurity.com/files/119218/wpreflexgallery-shell.txt
    </reference>
  </hash>
```

WPScan – Signatures actives

```
def registration_enabled?  
  resp = Browser.get(registration_url)  
  # redirect only on non multi sites  
  if resp.code == 302 and resp.headers_hash['location'] =~ /wp-login\.php\?registration=disabled/i  
    enabled = false  
  # multi site registration form  
  elsif resp.code == 200 and resp.body =~ /<form id="setupform" method="post" action="[^"]*wp-signup\.php[^"]*">/i  
    enabled = true  
  # normal registration form  
  elsif resp.code == 200 and resp.body =~ /<form name="registerform" id="registerform" action="[^"]*wp-login\.php[^"]*" /i  
    enabled = true  
  # registration disabled  
  else  
    enabled = false  
  end  
  enabled  
end
```

WPScan – Signatures actives

```
$wp-content$/themes/13floor/timthumb.php  
$wp-content$/themes/13floor/tools/timthumb.php  
$wp-content$/themes/8cells/timthumb.php  
$wp-content$/themes/8Cells/timthumb.php  
$wp-content$/themes/8q/scripts/thumb.php  
$wp-content$/themes/8q/scripts/timthumb.php  
$wp-content$/themes/abstract/custom/thumb.php  
$wp-content$/themes/abstract/custom/timthumb.php
```

Limites de WPScan

- S'applique uniquement à WordPress;
- Notion de contexte encore limitée;

```
{
  "4.3": {
    "release_date": "2015-08-18",
    "changelog_url": "https://codex.wordpress.org/Version_4.3",
    "vulnerabilities": [
      {
        "id": 8186,
        "title": "WordPress <= 4.3 - Authenticated Shortcode Tags Cross-Site Scripting (XSS)",
        "created_at": "2015-09-15T15:27:07.000Z",
        "updated_at": "2015-09-21T12:58:32.000Z",
        "published_date": "2015-09-15T00:00:00.000Z",
        "references": {
          "url": [
            "https://wordpress.org/news/2015/09/wordpress-4-3-1/",
            "http://blog.checkpoint.com/2015/09/15/finding-vulnerabilities-in-core-wordpress-a-bug-hunters-trilogy-part-iii-ultimatum/",
            "http://blog.knownsec.com/2015/09/wordpress-vulnerability-analysis-cve-2015-5714-cve-2015-5715/"
          ],
          "cve": [
            "2015-5714"
          ]
        },
        "vuln_type": "XSS",
        "fixed_in": "4.3.1"
      },
      {
        "id": 8187,
        "title": "WordPress <= 4.3 - User List Table Cross-Site Scripting (XSS)",
        "created_at": "2015-09-15T15:30:07.000Z",
        "updated_at": "2015-10-28T07:31:15.000Z",
        "published_date": "2015-09-15T00:00:00.000Z",
        "references": {
          "url": [
            "https://wordpress.org/news/2015/09/wordpress-4-3-1/",
            "https://github.com/WordPress/WordPress/commit/f91a5fd10ea7245e5b41e288624819a37adf290a"
          ],

```




À la recherche de signatures « passives »

Noms d'éléments

- Les Framework de développements nomment les éléments d'une façon spécifique;
 - Identifiant des éléments HTML
 - « Name » des input fields

```
<a id="ctl00_ctl00_PF_HyperLink24" c  
<a id="ctl00_ctl00_PF_HyperLink25" c  
<a id="ctl00_ctl00_PF_HyperLink26" c  
<a id="ctl00_ctl00_PF_HyperLink27" c  
<a id="ctl00_ctl00_PF_HyperLink28" c  
<a id="ctl00_ctl00_PF_HyperLink29" c  
<a id="ctl00_ctl00_PF_HyperLink30" c  
<a id="ctl00_ctl00_PF_HyperLink31" c  
<a id="ctl00_ctl00_PF_HyperLink32" c  
<a id="ctl00_ctl00_PF_HyperLink33" c
```

Noms d'éléments

- Les Framework de développements nomment les éléments d'une façon spécifique;
 - Identifiant des éléments HTML
 - « Name » des input fields

```
name="tx_stsphinxsearch_search[selectedIndex]">
```

Noms d'éléments

- Les Framework de développements nomment les éléments d'une façon spécifique;
 - Identifiant des éléments HTML
 - « Name » des input fields

```
<iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1'  
style="position:absolute;width:0;height:0;border:0"></iframe>
```

Commentaires

- Les commentaires contiennent souvent des informations sur les technologies utilisées;
- Commentaires :
 - HTML
 - JavaScript
 - CSS

```
/**
 * OK
 *
 * Open a jackrabbit file
 *
 * @param uuid
 *         UUID of the file
 * @param fileName
 *         Filename
 */
```

Classes CSS

Layout Helpers

- `.ui-helper-hidden`: Hides content visually and from assistive technologies, such as screen readers.
- `.ui-helper-hidden-accessible`: Hides content visually, but leaves it available to assistive technologies.
- `.ui-helper-reset`: A basic style reset for DOM nodes. Resets padding, margins, text-decoration, list-style, etc.
- `.ui-helper-clearfix`: Applies float wrapping properties to parent elements.
- `.ui-front`: Applies z-index to manage the stacking of multiple widgets on the screen. See the page about [stacking elements](#) for more details.

Favicon, images, code JavaScript, ...

- Principe présent dans certains outils;
- Peu être étendu à tout type de fichiers
 - Images
 - JavaScript
 - CSS
 - Etc.

OWASP favicon database

favicon database in wiki format (licensed under CC BY license), feel free to contribute directly to this wiki by editing this page Versions in brackets means that they have been seen on that version, but we don't have correct version span for particular favicon, feel free to contribute that as well.

```
6399cc480d494b1fcd7d16c42b1c11b:penguin
09b565a51e14b721a323f0ba44b2982a:Google web server
506190fc55ceaa132f1bc305ed8472ca:SocialText
2cc15cfae55e2bb2d85b57e5b5bc3371:PHPwiki (1.3.14) / gforge (4.6.99+svn6496) -
389a8816c5b87685de7d8d5fec96c85b:XOOPS cms
f1876a80546b3986dbb79bad727b0374:NetScreen WebUI or 3Com Router
226ffc5e483b85ec261654fe255e60be:Netscape 4.1
b25dbe60830705d98ba3aaf0568c456a:Netscape iPlanet 6.0
41e2c893098b3ed9fc14b821a2e14e73:Netscape 6.0 (AOL)
a28ebcac852795fe30d8e99a23d377c1:SunOne 6.1
71e30c507ca3fa005e2d1322a5aa8fb2:Apache on Redhat
d41d8cd98f00b204e9800998ecf8427e:Zero byte favicon
```

Source image :

Favicon, images, code JavaScript, ...

- Principe présent dans certains outils;
- Peu être étendu à tout type de fichiers
 - Images
 - JavaScript
 - CSS
 - Etc.



Source image :

Favicon, images, code JavaScript, ...

- Principe présent dans certains outils;
- Peu être étendu à tout type de fichiers
 - Images
 - JavaScript
 - CSS
 - Etc.

```
/*!
 * Piwik - free/libre analytics platform
 *
 * JavaScript tracking client
 *
 * @link http://piwik.org
 * @source https://github.com/piwik/piwik/blob/master/js/piwik.js
 * @license http://piwik.org/free-software/bsd/ BSD-3 Clause (also in js/LICENSE.txt)
 * @license magnet:?xt=urn:btih:c80d50af7d3db9be66a4d0a86db0286e4fd33292&dn=bsd-3-clause.txt BSD-3-Clause
 */
if(typeof JSON2!="object"){JSON2=window.JSON||{}}(function(){function d(f){return f<10?"0"+f:function l(
function a(f){i.lastIndex=0;return i.test(f)?''+f.replace(i,function(m){var n=k[m];return typeof n=="stri
return t}}if(typeof JSON2.stringify!="function"){JSON2.stringify=function(o,m,n){var f;j="";b="";if(typeof
return typeof f=="function"?m({":n",""):n}throw new SyntaxError("JSON2.parse")}}})();if(typeof _paq!="ob
}while(W.getTimeAlias(<j))}function P(){var W;if(!p){p=true;O("load");for(W=0;W<E.length;W++){E[W]()}}retu
try{W=G.top.document.referrer}catch(Y){if(G.parent){try{W=G.parent.document.referrer}catch(X){W=""}}if(W=
break;case 3:ap=am.charCodeAt(X-3)<<24|am.charCodeAt(X-2)<<16|am.charCodeAt(X-1)<<8|128;break)af.push(ap);w
}function N(Y,W,X){if(Y=="translate.googleusercontent.com"){if(X=="")X=W;W=I(W,"u");Y=c(W)}else{if(Y=="
}function W(aa,ab){if(G.getComputedStyle){return u.defaultView.getComputedStyle(aa,null)[ab]}if(aa.currentS
}var Q={htmlCollectionToArray:function(Y){var W=[];X;if(!Y||!Y.length){return W}for(X=0;X<Y.length;X++){W.p
}if(!aa||!aa.attributes){return}var Z=(typeof aa.attributes[Y]);if("undefined"===Z){return}if(aa.attributes
}if(this.hasNodeAttribute(Y,X)){return Y}var W=this.findNodesHavingAttribute(Y,X);if(W&W.length){return W[
var Y=z(Z,W);return Y!==-1},setAnyAttribute:function(X,W,Y){if(!X||!W){return}if(X.setAttribute){X.setAttri
}}X=Q.makeNodesUnique(X);return X},findParentContentNode:function(X){if(!X){return}var Y=X;var W=0;while(Y&
}var W=this.findContentPiece(X);if(W){return this.removeDomainIfIsInLink(W)}if(Q.hasNodeAttributeWithValue(
if(Q.hasNodeAttributeWithValue(W,"href")){X=Q.getAttributeValueFromNode(W,"href");return this.toAbsoluteUrl
}}var ac=Q.findNodesByTagName(aa,"embed");if(ac&ac.length){return this.findMediaUrlInNode(ac[0])}}},trim:
},buildContentBlock:function(Y){if(!Y){return}var W=this.findContentName(Y);var X=this.findContentPiece(Y);
}if(X.search(/^\/\//)!=-1){return this.getLocation().origin+X}var W="(.*/)";var Y=this.getLocation().origin+
G.name+W+"###"+ac+"###"+X}var ab=G.name.split("###");return ab.length==3&&ab[0]==W}function M(X,ac,Z){var
function bS(cv,cs,cr,cu,cq,ct){if(ao){return}var cp;if(cr){cp=new Date();cp.setTime(cp.getTime()+cr)}u.cook
}};cq.src=aa+(aa.indexOf("?")<0?"?":"&")+cp}function bT(cq,ct,cp){if(!w(cp)||null===cp){cp=true}try{var cs=
return}if(bf===false){var cs=800;bf=cp+cs}ct()function a3(cq,cp,cr){if(!b8&&cq){aH(function(){if(bD===POS
}return ct}if(a6.length){cs=a6}else{if("0"===ae()){cs=""}else{cs=ce()}}ct=["1",cs,cp,0,cp,"",""];return ct}
ao=false;var cp=["id","ses","cvar","ref"];var cq,cs;for(cq=0;cq<cp.length;cq++){cs=bR(cp[cq]);if(0!=av(cs)
}}}
```

Objets sérialisés

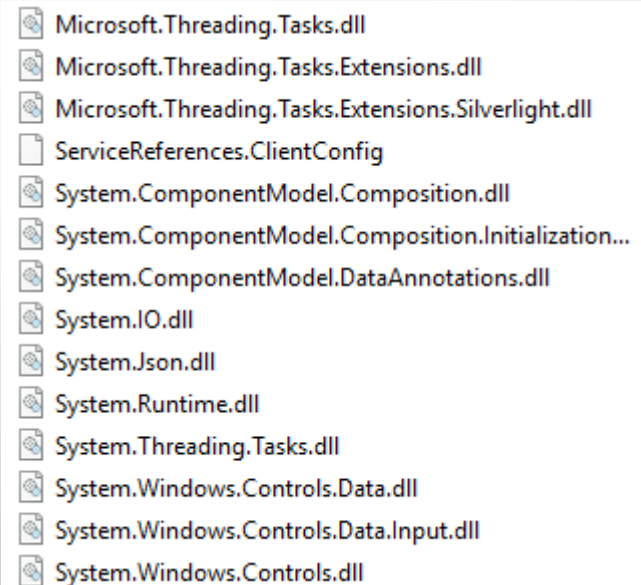
/wEPZwUPOGQzM2Y3M2lwNzg1MzkyWbw/wYx/I
YvG81uN4hyb6lOalw=

- L'utilisation d'objets sérialisés est courante;
- La nature de l'objet nous renseigne sur la technologie utilisée;
- Ces objets doivent contenir des informations de version pour pouvoir être dé-sérialisé;

```
ViewState
├── Version
│   └── 2
├── VersionString
│   └── ASP.Net 2.X
├── MAC
│   └── 59BC3FC18C7F218BC6F35B8DE21C9BEA539A235C
└── ViewStateDeserialized
    ├── System.Web.UI.Pair
    │   ├── System.Boolean
    │   │   └── True
    │   └── System.String
    │       └── 8d33f73b0785392
```

Contenu riche

- Le contenu riche décompiler donne énormément d'informations :
 - Silverlight (<http://ilspy.net/>)
 - Java (<http://jd.benow.ca/>)
 - Flash (<http://www.swftools.org/>)



A screenshot of a decompiled rich content file, likely a Silverlight application, showing a list of embedded resources. The list includes various .dll files from Microsoft and System namespaces, as well as a .ClientConfig file. The items are listed in a vertical column, each preceded by a small icon representing a file type.

- Microsoft.Threading.Tasks.dll
- Microsoft.Threading.Tasks.Extensions.dll
- Microsoft.Threading.Tasks.Extensions.Silverlight.dll
- ServiceReferences.ClientConfig
- System.ComponentModel.Composition.dll
- System.ComponentModel.Composition.Initialization...
- System.ComponentModel.DataAnnotations.dll
- System.IO.dll
- System.Json.dll
- System.Runtime.dll
- System.Threading.Tasks.dll
- System.Windows.Controls.Data.dll
- System.Windows.Controls.Data.Input.dll
- System.Windows.Controls.dll

Métadonnées

- Les outils de génération de contenu laissent des traces :
 - Génération de rapports (PDF, Word, Excel, ...)
 - Génération d'images

Propriétés ▾	
Taille	271 Ko
Pages	
Mots	
Temps total d'édition	116151 minute(s)
Titre	Struts2 IDE - WTP XM...
Ba	
Co	
M	
État	Aucun
Catégories	Aucun
Objet	Aucun
Répertoire web	Aucun
Société	Aucun

Titre
Struts2 IDE - WTP XML Search Engine

Rendu DOM

- L'analyse « statique » de la réponse a ses limites;
- Principe utilisé de façon limité par Wappalyzer;

```
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage"
google.j.b=(!!location.hash&&!!location.hash.match(['#&'])(q|fp)=|tbs=r
|| (google.j.qbp==1); (function() {google.c={c:{a:true,d:false,i:false,m:t
h|b.ctrlKey|b.shiftKey|b.altKey|b.metaKey|H(m)&&32==f}|| (h=m.tag|
t[u];if(!n){for(var n={},y=u.split(ea),z=0,fa=y?y.length:0;z<fa;z++){ve
(g.type||g.tagName).toUpperCase(), (g=32==(b.which|b.keyCode|b.key)&&'
"srcElement"!=p&&"target"!=p&&(c[p]=b[p]);c.type="mouseover"==b.type?
.gbii::before{content:url(/lh3.googleusercontent.com/-46ZKhHJuifY/AA
.gbii{background-image:url(/lh3.googleusercontent.com/-46ZKhHJuifY/AA
</style><style data-jiis="cc" id="gstyle">html,body{height:100%;margin:
(window['gbar']=window['gbar']||{}). _CONFIG=[[0,"www.gstatic.com","og
try{
var aa,ca,da,ba,ea,fa,ga,ha,ia,pa,qa;aa="undefined"!=typeof window&&win
ga=function(a,c){a instanceof String&&(a=String(a));var d=0;ca();ea();v
ia=function(a){if(null==this)throw new TypeError("The 'this' value for
.n=function(a){return void 0!=a};_q=function(a,c){for(var d=a.split
_.la=function(a){var c=typeof a;if("object"==c)if(a){if(a instanceof A
else if("function"==c&&"undefined"==typeof a.call)return"object";return
qa=function(a,c,d){if(!a)throw Error();if(2<arguments.length){var e=Arr
_.x=function(a,c){var d=a.split(".");e=_m;d[0]in e||!e.execScript||e.e
var ra=function(a,c,d){this.A=a;this.o=!1;this.b=c;this.w=d};ra.prototy
var sa=function(a){_.z.call(this);this.w=a;this.b=[];this.o={}};_.y(sa,
sa.prototype.Sa=function(){for(var a=this.b.length,c=this.b,d=[],e=0;e<
_.ta=function(a){if(Error.captureStackTrace>Error.captureStackTrace(thi
_.wa=function(a,c){for(var d=0,e=(0,_.ua)(String(a)).split("."),f=(0,_.
_.xa=Array.prototype.indexOf?function(a,c,d){return Array.prototype.inc
_.za=Array.prototype.filter?function(a,c,d){return Array.prototype.filt
_.Ba=Array.prototype.reduce?function(a,c,d,e){e&&(c=(0,_.u)(c,e));retur
var Ka;_.Da=function(){this.b={};this.o={}};_.ka(_.Da);_.Fa=function(a,
var Ma;_.La="bbh bbr bbs has prm sngw so".split(" ");Ma=new sa(_.m);_.l
for(var Na="addExtraLink addLink aomc asmc close cp.c cp.l cp.me cp.ml
a:{var Sa=_.m.navigator;if(Sa){var Ta=Sa.userAgent;if(Ta){_.Ra=Ta;brea
jb=function(){var a=_.m.document;return a?a.documentMode:void 0};a:{var
_.ub=_.A("Firefox");_.vb=_.Va()||_.A("iPod");_.wb=_.A("iPad");_.xb=_.A
var Eb=function(a,c,d){if(null==c)d.push("null");else if("object"==type
d).break;case "number":d.push((0,window.isFinite)(c)?c:(0,window.isNaN)
```

Rendu DOM

- L'analyse « statique » de la réponse a ses limites;
- Principe utilisé de façon limité par Wappalyzer;

```
<!DOCTYPE html>
<html lang="en-CA" itemtype="http://schema.org/WebPage" itemscope="">
  <head>
    <meta itemprop="image" content="/images/branding/googleg/1x/googleg_standard_color_128dp.png">
    <link rel="shortcut icon" href="/images/branding/product/ico/googleg_lodp.ico">
    <meta id="mref" name="referrer" content="origin">
    <title>Google</title>
    <script src="https://apis.google.com/_scs/abc-static/_/js/k=gapi.gapi.en.PQWOXwGAYXQ.O
/m=gapi_iframes,googleapis_client,iframes_styles_slide_menu,plusone/rt=j/sv=1/d=1/ed=1/rs=AHpOc
SsKefX_tnkYaztI7tux9JZAkUgw/cb=gapi.loaded_0" async="">
    <script>
    <style>
    <style id="gstyle" data-jiiis="cc">
    <script>
    <style type="text/css">
    <script async="" type="text/javascript" charset="UTF-8" src="//www.gstatic.com/og/_/js
/k=og.og2.en_US.BdrRkszXe6w.O/rt=j/m=drt,def/exm=in,fot/d=1/ed=1/rs=AA2YrTuzZXZ4J84ZILm_32EGgnf
/m=lq/excm=in,fot/d=1/ed=1/rs=AA2YrTtuaFHeUPM6LnuKSrhjMA6Uw17fHg">
    <link rel="stylesheet" type="text/css" href="//www.gstatic.com/og/_/ss/k=og.og2.-wa95qi4vz3dc.I
/m=lq/excm=in,fot/d=1/ed=1/rs=AA2YrTtuaFHeUPM6LnuKSrhjMA6Uw17fHg">
    <script async="" type="text/javascript" charset="UTF-8" src="//www.gstatic.com/og/_/js
/k=og.og2.en_US.BdrRkszXe6w.O/rt=j/m=lat/exm=in,fot,drt,def/d=1/ed=1
/rs=AA2YrTuzZXZ4J84ZILm_32EGgnfxNwMCTQ">
    <style type="text/css">
  </head>
  <body id="gsr" class="hp vasq" onload="try{if(!google.j.b){document.f&#64;document.f.q.focus();docume
document.gbqf.q.focus();}}catch(e){}if(document.images)new Image().src='/images/nav_logo242.png'">
    <div id="viewport" class="ctr-p">
      <div id="doc-info" data-jiiis="cc"></div>
      <div id="cst" data-jiiis="cc">
        <style>
```

Rendu DOM

- L'analyse « statique » de la réponse a ses limites;
- Principe utilisé de façon limité par Wappalyzer;

+ DrawCurve	Object { Class="DrawCurve", \$bp=true, isFrameworkClass=true, plus... }
+ DrawDiamond	Object { Class="DrawDiamond", \$bp=true, isFrameworkClass=true, plus... }
+ DrawGroup	Object { Class="DrawGroup", \$bp=true, isFrameworkClass=true, plus... }
+ DrawImage	Object { Class="DrawImage", \$bp=true, isFrameworkClass=true, plus... }
+ DrawItem	Object { Class="DrawItem", \$bp=true, isFrameworkClass=true, plus... }
+ DrawItemEditProxy	Object { Class="DrawItemEditProxy", \$bp=true, isFrameworkClass=true, plus... }
+ DrawKnob	Object { Class="DrawKnob", \$bp=true, isFrameworkClass=true, plus... }
+ DrawLabel	Object { Class="DrawLabel", \$bp=true, isFrameworkClass=true, plus... }
+ DrawLabelEditProxy	Object { Class="DrawLabelEditProxy", \$bp=true, isFrameworkClass=true, plus... }
+ DrawLine	Object { Class="DrawLine", \$bp=true, isFrameworkClass=true, plus... }
+ DrawLinePath	Object { Class="DrawLinePath", \$bp=true, isFrameworkClass=true, plus... }
+ DrawOval	Object { Class="DrawOval", \$bp=true, isFrameworkClass=true, plus... }
+ DrawPane	Object { Class="DrawPane", \$bp=true, isFrameworkClass=true, plus... }
+ DrawPaneEditProxy	Object { Class="DrawPaneEditProxy", \$bp=true, isFrameworkClass=true, plus... }
+ DrawPath	Object { Class="DrawPath", \$bp=true, isFrameworkClass=true, plus... }
+ DrawPolygon	Object { Class="DrawPolygon", \$bp=true, isFrameworkClass=true, plus... }



À la recherche de signatures « actives »

Fichiers de politiques

- Les fichiers de politiques servent à donner des instructions aux utilisateurs;
- Ils donnent souvent trop d'informations;
- Exemples de fichiers de politiques:
 - Robots.txt
 - crossdomain.xml
 - clientaccesspolicy.xml

Source image : <https://www.drupal.org/robots.txt>

```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html
#
# For syntax checking, see:
# http://www.frobe.com/robots-txt-check

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
```

Pages d'erreurs

- Les pages d'erreurs par défaut permettent d'identifier les technologies;
- Les erreurs 404 sont faciles à générer :
 - www.example.com/jhkjlhqwvebqnwjdev6785213713vhjg87r3b.html

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

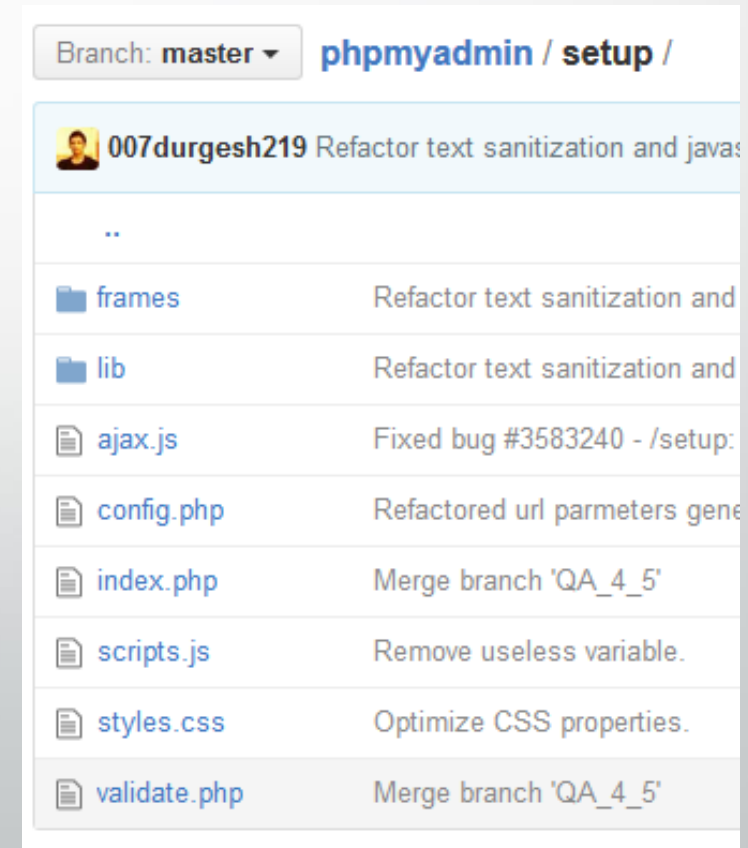
Pages d'erreurs

- Les pages d'erreurs par défaut permettent d'identifier les technologies;
- Les erreurs 404 sont faciles à générer :
 - www.example.com/jhkjlhqwvebqnwjdev6785213713vhjg87r3b.html

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.

Structure de répertoire

- Les technologies ont une structure de répertoire qui leur être propre;
- Les ressources référencées varient d'une version à l'autre;
- Etc.



Structure de répertoire

- Les technologies ont une structure de répertoire qui leur être propre;
- Les ressources référencées varient d'une version à l'autre;
- Etc.

```
git clone https://github.com/phpmyadmin/phpmyadmin  
Get-ChildItem .\phpmyadmin -Name -Recurse |  
    % { "http://www.example.com/" + $_.replace("\", "/") }
```

Structure de répertoire

- Les technologies ont une structure de répertoire qui leur être propre;
- Les ressources référencées varient d'une version à l'autre;
- Etc.

TYPO3 CMS

TYPO3 is an open source PHP based web content management system released under the GNU GPL. TYPO3 is copyright (c) 1999-2013 by Kasper Skaarhøj.

This document provides a basic introduction to TYPO3.

Getting Started

TYPO3 requires a webserver with PHP and a database (MySQL recommended). Accessing the backend through a supported browser.

Please see the INSTALL.md in this folder in order to set up a basic TYPO3 installation on your webserver.

What is TYPO3?

TYPO3 is a free and open source Content Management Framework. It is released under the GNU General Public License. It can run on several web servers, such as Apache or IIS, on top of many operating systems, among them Linux, Microsoft Windows, FreeBSD or MacOS X.

TYPO3 was initially authored by Kasper Skårhøj and is now further developed by a community of Active Contributors around a small TYPO3 CMS Team.

To get more info about the GPL license, visit
<http://www.opensource.org/licenses/gpl-license.php>

What is a Content Management Framework?

A Content Management Framework is more than just a content management system, due to the separation of the streamlined core and optional plugins (extensions). TYPO3 has an open API that allows you to extend the frontend (web site) and/or backend (administration) functionalities.

The concept of extensions makes TYPO3 capable of being developed and used in almost any way you can imagine, either by using any of the many extensions which are available for download, or by writing your own.

Noms d'utilisateurs

- Les technologies ont souvent des noms d'utilisateurs par défaut;

1. Sourcefire - RNA Sensor

Method	HTTP
User ID	admin
Password	password
Level	Administrator

2. Sourcefire - RNA Sensor

Method	SSH/Console
User ID	root
Password	password
Level	Administrator



Pour une meilleure identification

Tenir compte du contexte

- Différents code de statut;
- Recherche de valeurs pour des URL précis;
- Recherche en fonction de l'emplacement;
- Contenu statique versus contenu « dynamique »;

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Tenir compte du contexte

- Différents code de statut;
- Recherche de valeurs pour des URL précis;
- Recherche en fonction de l'emplacement;
- Contenu statique versus contenu « dynamique »;

```
def registration_enabled?  
  resp = Browser.get(registration_url)  
  # redirect only on non multi sites  
  if resp.code == 302 and resp.headers_hash['location'] =~ /wp-login\.php\?registration=disabled/i  
    enabled = false  
  # multi site registration form  
  elsif resp.code == 200 and resp.body =~ /<form id="setupform" method="post" action="[^"]*wp-signup\.php[^"]*">/i  
    enabled = true  
  # normal registration form  
  elsif resp.code == 200 and resp.body =~ /<form name="registerform" id="registerform" action="[^"]*wp-login\.php[^"]*">/i  
    enabled = true  
  # registration disabled  
  else  
    enabled = false  
  end  
  enabled  
end
```

Tenir compte du contexte

- Différents code de statut;
- Recherche de valeurs pour des URL précis;
- Recherche en fonction de l'emplacement;
- Contenu statique versus contenu « dynamique »;

```
<iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1'  
style="position:absolute;width:0;height:0;border:0"></iframe>
```

Tenir compte du contexte

- Différents code de statut;
- Recherche de valeurs pour des URL précis;
- Recherche en fonction de l'emplacement;
- Contenu statique versus contenu « dynamique »;

```
<!DOCTYPE html>
<html lang="en-CA" itemtype="http://schema.org/WebPage" itemscope="">
  <head>
    <meta itemprop="image" content="/images/branding/googleg/1x/googleg_standard_color_128dp.png">
    <link rel="shortcut icon" href="/images/branding/product/ico/googleg_lodp.ico">
    <meta id="mref" name="referrer" content="origin">
    <title>Google</title>
    <script src="https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.PQWOXwGAYXQ.O
/m=gapi_iframes,googleapis_client,iframes_styles_slide_menu,plusone/rt=j/sv=1/d=1/ed=1/rs=AHpOc
SsKefX_tnkYaztI7tux9JZAkUgw/cb=gapi.loaded_0" async="">
    <script>
    <style>
    <style id="gstyle" data-jiiis="cc">
    <style>
    <script>
    <style type="text/css">
    <script async="" type="text/javascript" charset="UTF-8" src="//www.gstatic.com/og/_/js
/k=og.og2.en_US.BdrRkszXe6w.O/rt=j/m=drt,def/exm=in,fot/d=1/ed=1/rs=AA2YrTuzZXZ4J84ZILm_32EGgnf
    <link rel="stylesheet" type="text/css" href="//www.gstatic.com/og/_/ss/k=og.og2.-wa95qi4vz3dc.I
/m=lg/excm=in,fot/d=1/ed=1/rs=AA2YrTuzFHeUPM6LnuKSrhjMA6Uw17fHg">
    <script async="" type="text/javascript" charset="UTF-8" src="//www.gstatic.com/og/_/js
/k=og.og2.en_US.BdrRkszXe6w.O/rt=j/m=lat/exm=in,fot,drt,def/d=1/ed=1
/rs=AA2YrTuzZXZ4J84ZILm_32EGgnfxNwMCTQ">
    <style type="text/css">
  </head>
  <body id="gsr" class="hp vasq" onload="try{if(!google.j.b){document.f%$document.f.q.focus();docume
document.gbqf.q.focus();}}catch(e){}if(document.images)new Image().src='/images/nav_logo242.png'">
    <div id="viewport" class="ctr-p">
      <div id="doc-info" data-jiiis="cc"></div>
      <div id="cst" data-jiiis="cc">
        <style>
```

Utiliser le bon formalisme de recherche

- Images, favicon, librairies JavaScript

OWASP favicon database

favicon database in wiki format (licensed under CC BY license), feel free to contribute directly to this wiki by editing this page Versions in brackets means that they have been seen on that version, but we don't have correct version span for particular favicon, feel free to contribute that as well.

```
6399cc480d494bf1fcd7d16c42b1c11b:penguin
09b565a51e14b721a323f0ba44b2982a:Google web server
506190fc55ceaa132f1bc305ed8472ca:SocialText
2cc15cfae55e2bb2d85b57e5b5bc3371:PHPwiki (1.3.14) / gforge (4.6.99+svn6496) -
389a8816c5b87685de7d8d5fec96c85b:XOOPS cms
f1876a80546b3986dbb79bad727b0374:NetScreen WebUI or 3Com Router
226ffc5e483b85ec261654fe255e60be:Netscape 4.1
b25dbe60830705d98ba3aaf0568c456a:Netscape iPlanet 6.0
41e2c893098b3ed9fc14b821a2e14e73:Netscape 6.0 (AOL)
a28ebcac852795fe30d8e99a23d377c1:SunOne 6.1
71e30c507ca3fa005e2d1322a5aa8fb2:Apache on Redhat
d41d8cd98f00b204e9800998ecf8427e:Zero byte favicon
```

Utiliser le bon formalisme de recherche

- Images, favicon, librairies JavaScript
- HTML & XML

Path Expression	Result
bookstore	Selects all nodes with the name "bookstore"
/bookstore	Selects the root element bookstore Note: If the path starts with a slash (/) it always represents an absolute path to an element!
bookstore/book	Selects all book elements that are children of bookstore
//book	Selects all book elements no matter where they are in the document
bookstore//book	Selects all book elements that are descendant of the bookstore element, no matter where they are under the bookstore element
//@lang	Selects all attributes that are named lang

Utiliser le bon formalisme de recherche

- Images, favicon, librairies JavaScript
- HTML & XML
- DOM document

Selector	Example	Example description
<u>.class</u>	.intro	Selects all elements with class="intro"
<u>#id</u>	#firstname	Selects the element with id="firstname"
<u>*</u>	*	Selects all elements
<u>element</u>	p	Selects all <p> elements
<u>element,element</u>	div, p	Selects all <div> elements and all <p> elements
<u>element element</u>	div p	Selects all <p> elements inside <div> elements
<u>element>element</u>	div > p	Selects all <p> elements where the parent is a <div> element
<u>element+element</u>	div + p	Selects all <p> elements that are placed immediately after <div> elements
<u>element1~element2</u>	p ~ ul	Selects every element that are preceded by a <p> element
<u>[attribute]</u>	[target]	Selects all elements with a target attribute

Utiliser le bon formalisme de recherche

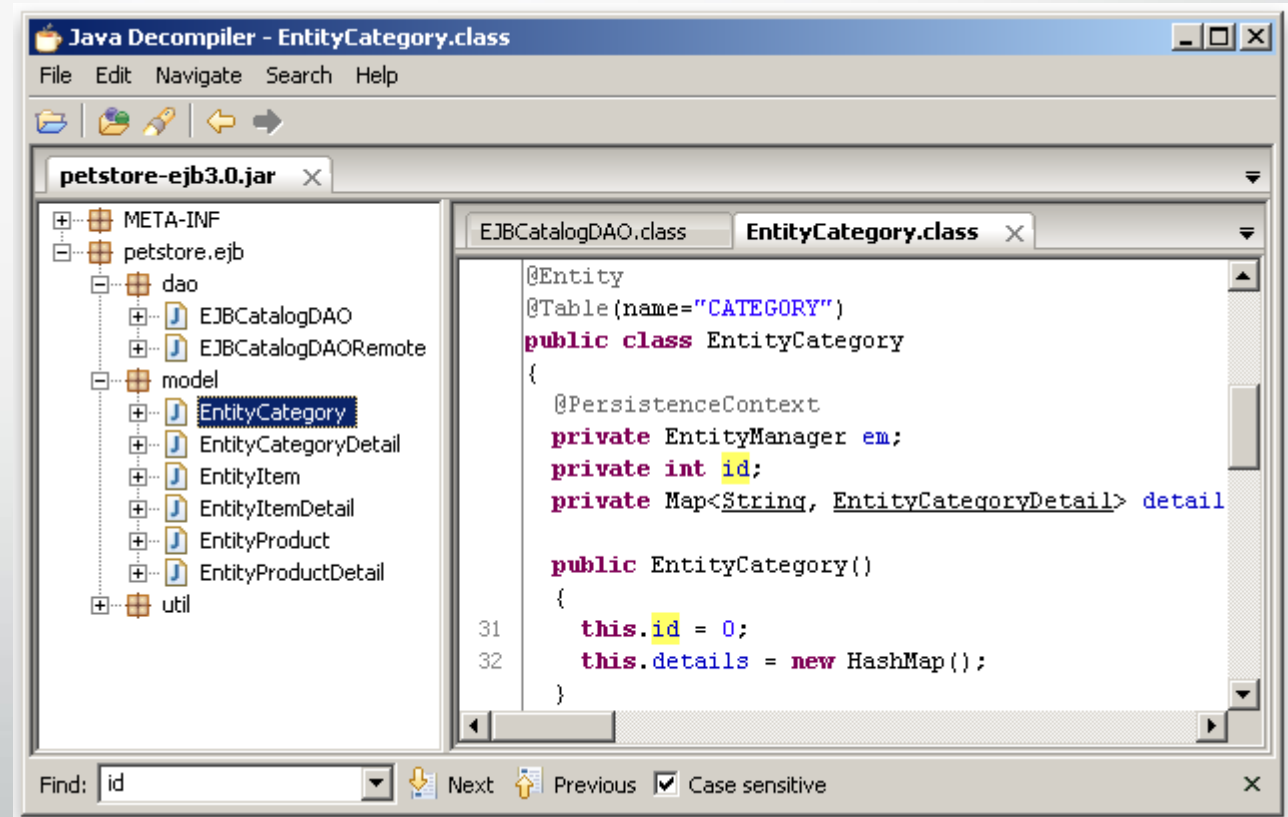
- Images, favicon, librairies JavaScript
- HTML & XML
- DOM document
- JavaScript

```
1 var letterRE = new RegExp('[a-zA-Z]', 'g'),  
2   digitRE = RegExp('[0-9]');  
3  
4 // from jQuery  
5  
6 var rformElems = /^(?:input|select|textarea)$/i,  
7   rkeyEvent = /^key/,  
8   rmouseEvent = /^(?:mouse|contextmenu)|click/,  
9   rfocusMorph = /^(?:focusin|focus|focusout|blur)$/i,  
10  rtypenamespace = /^([^.]*)(?:\.(.+)|)$/i;  
11  
12 // from Lo-Dash  
13  
14 var reEscapedHtml = /&(?:(amp|lt|gt|quot|#39));/g;  
15 var reEmptyStringLeading = /\b__p \+= '';/g,  
16   reEmptyStringMiddle = /\b(__p \+=) '' \+/g,  
17   reEmptyStringTrailing = /(__e\((.*?\))\b__t\)) \+=\n'';/g;  
18
```

Total regular expressions: 11

Utiliser le bon formalisme de recherche

- Images, favicon, librairies JavaScript
- HTML & XML
- DOM document
- JavaScript
- Contenu riche



Les signatures sont partout

- À peu près tout peut servir de signature;
- La taille de la banque de signatures est primordiale;
- Wappalyzer;
- Nikto ;
- WPScan;
- OWASP Favicon database;
- Default passwords database;
- Etc.

Les signatures sont partout

- À peu près tout peut servir de signature;
- La taille de la banque de signatures est primordiale;
- Toutes seules elles ne « servent » à rien.

The Exploit-Database Git Repository

This is the official repository of [The Exploit Database](#), a project sponsored by [Offensive Security](#).

The Exploit Database is an archive of public exploits and corresponding vulnerable software, developed by penetration testers and vulnerability researchers. Its aim is to serve as the most comprehensive collection of exploits gathered through direct submissions, mailing lists, and other public sources, and present them in a free and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than a binary exploits repository, making it a valuable resource for those who need actionable data right away.

This repository is updated daily with the most recently added submissions. Any additional resources can be found in the [binary exploits repository](#).

Projet personnel

- Indexer les communications dans une base de données NoSQL;

ZAP API UI

Component: core

View:messages

Gets the HTTP messages sent by ZAP, request and response

Output format

baseurl

start

count

Projet personnel

- Indexer les communications dans une base de données NoSQL;

```
{
  "_index" : "messages",
  "_type" : "request",
  "_id" : "1",
  "_version" : 2,
  "found" : true,
  "_source" : {
    "request" : {
      "start_line" : {
        "method" : "GET",
        "raw_url" : "http://nym1-ib.adnxs.com
/vevent?e=wqT_3QLhAqhhAQAAAawDWAAUBCKag4rkFEPG1h4C
jIgASotCQAACQIAEQkHLAAAGa5H4XoULidAIRESACKRCfCKMN
AHYBaABWqgBALABALgBAsABAsgBANABANgBAOABAPABAPoBCU
S9mciljYS8_Y29icmFuZD1kZWxsMTMubQke8Homb2NpZD1ERU
MADrALIAwDYA5T_EOADAogDAPgDAYAEAJIEBC90dGqYBACiBA
AdsgQICAAQABgAIAc4BADABADIBAA.&s=050ea2eadde7a263
%2Fwww.msn.com%2Ffr-ca%2F%3Fcobrand%3Ddell113.msn.
pd=28.24&d=273.29&ud=0&id=13.43&ic=2&d0=15.42&d25
mpy=0&px=518&py=175&bw=311&bh=166&sf=1&sw=1680&sh
tv=view5-1&ua=ie11&pl=win&x=1463324714273405585,3
      "parsed_url" : {
        "protocol" : "http:",
        "slashes" : true,
        "auth" : null,
        "host" : "nym1-ib.adnxs.com",
        "port" : null,
        "hostname" : "nym1-ib.adnxs.com",
        "hash" : null,
        "search" : "?e=wqT_3QLhAqhhAQAAAawDWAAUB
jIgASotCQAACQIAEQkHLAAAGa5H4XoULidAIRESACKRCfCKMN
AHYBaABWqgBALABALgBAsABAsgBANABANgBAOABAPABAPoBCU
```

Projet personnel

- Indexer les communications dans une base de données NoSQL;

```
request.start_line.parsed_url.query.name
```

Projet personnel

- Indexer les communications dans une base de données NoSQL;

```
{
  "_index" : "messages",
  "_type" : "request",
  "_id" : "1",
  "_version" : 2,
  "found" : true,
  "_source" : {
    "request" : {
      "start_line" : {
        "parsed_url" : {
          "query" : [ {
            "name" : "e"
          }, {
            "name" : "s"
          }, {
            "name" : "referrer"
          }, {
            "name" : "type"
          }, {
            "name" : "nvt"
          }, {
            "name" : "pd"
          }, {
            "name" : "d"
          }, {
            "name" : "ud"
          }, {
            "name" : "id"
          }, {
            "name" : "ic"
          }, {
            "name" : "d0"
          }
        ]
      }
    }
  }
}
```



Questions ?