

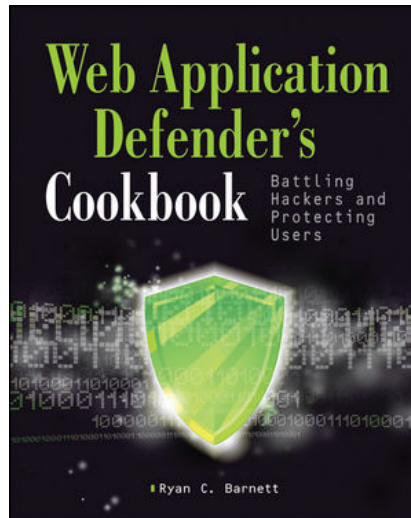


ModSecurity as Universal Cross-platform Web Protection Tool

Ryan Barnett
Greg Wroblewski

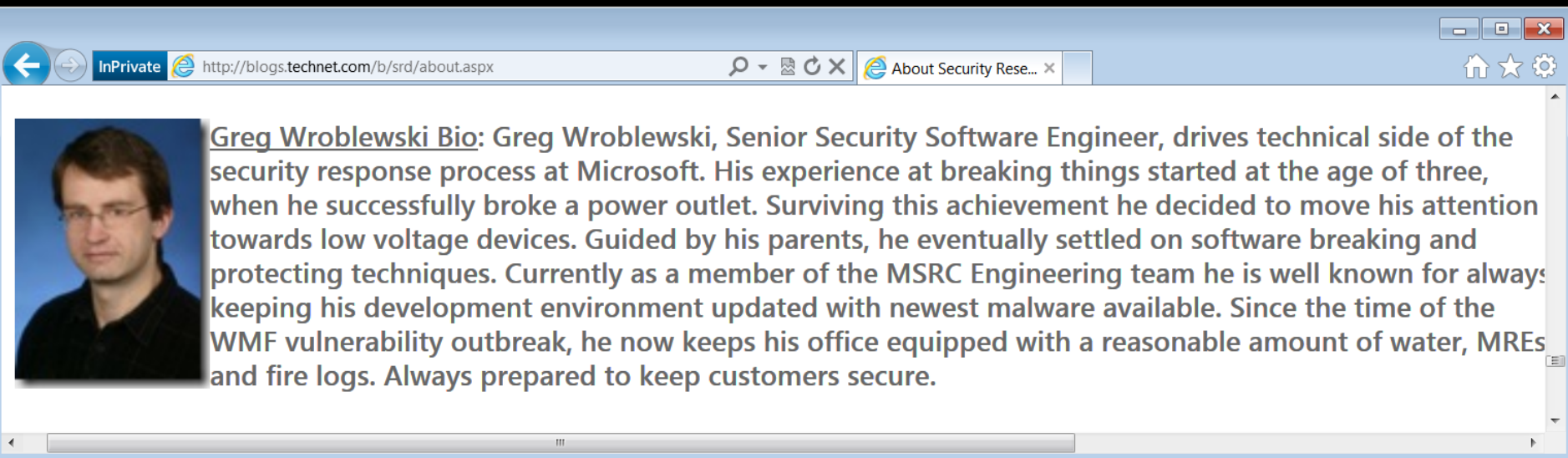
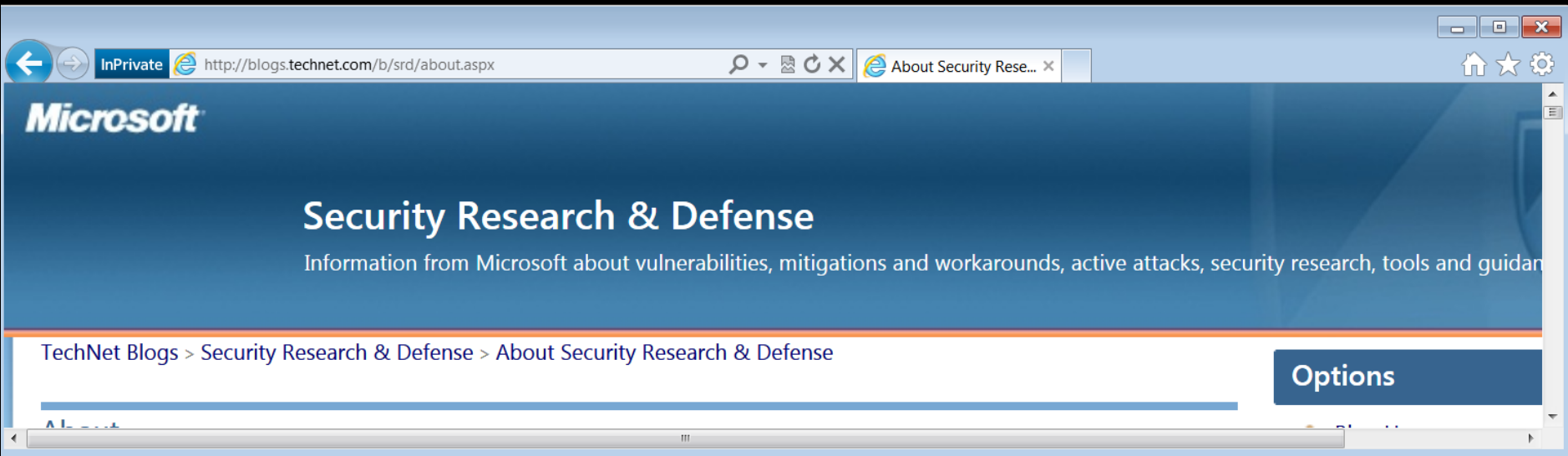


modsecurity
Open Source Web Application Firewall





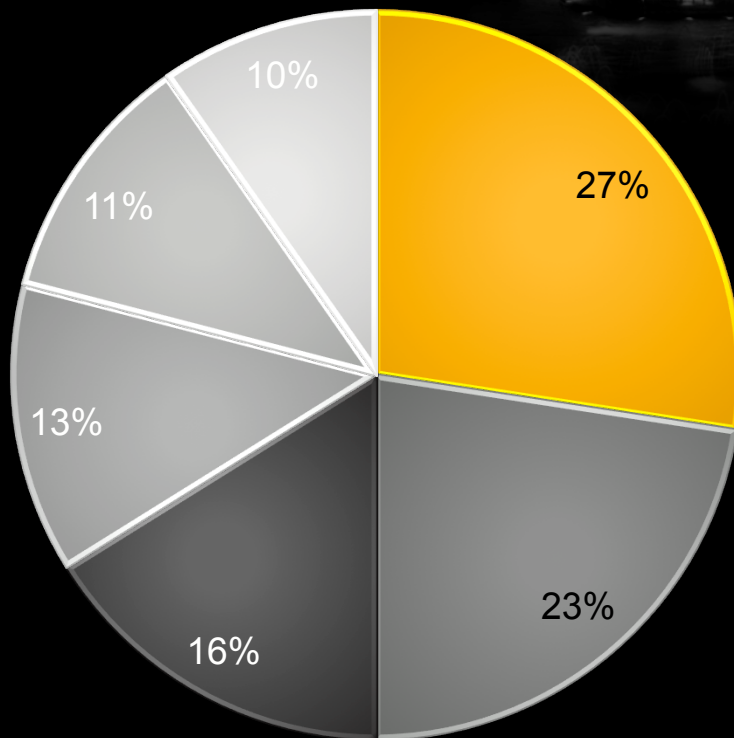
blackhat
USA 2012





**WEB APPLICATIONS ARE HIGHLY
TARGETED**

Source Code Fix Challenges



- Lack of Resources
- 3rd Party Code
- Outsourced Code
- Insufficient Technical Skill
- Insufficient Contract Scope
- Cost is Too High

Source: OWASP Web Application Virtual Patching Survey



WAIT FOR IT

.....Wait for it.....



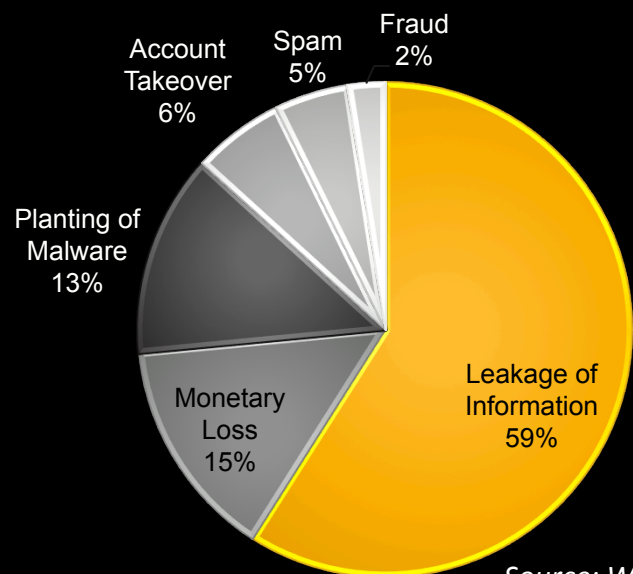
WHID

Web Hacking Incident Database

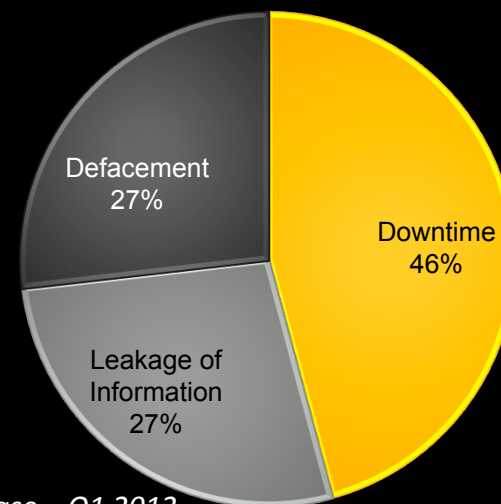
**Hackers Breach Credit Card Processor;
50K Cards Compromised**

CIA site downed as Anonymous claims attack

Profit



Hacktivism



Source: WASC Web Hacking Incident Database – Q1 2012



blackhat
USA 2012

WHY MODSECURITY?



Virtual Patching Definition:

A security policy enforcement layer which prevents the exploitation of a known vulnerability.

ModSecurity as Virtual Patching Tool

- Mature, well tested WAF module
 - Project is 10 years old
 - Protecting millions of websites
 - >275k source code downloads
- Rich feature set, spanning both mitigation and audit
- Significant community support
- Non-viral open source license
- OWASP Core Rule Set providing general protection

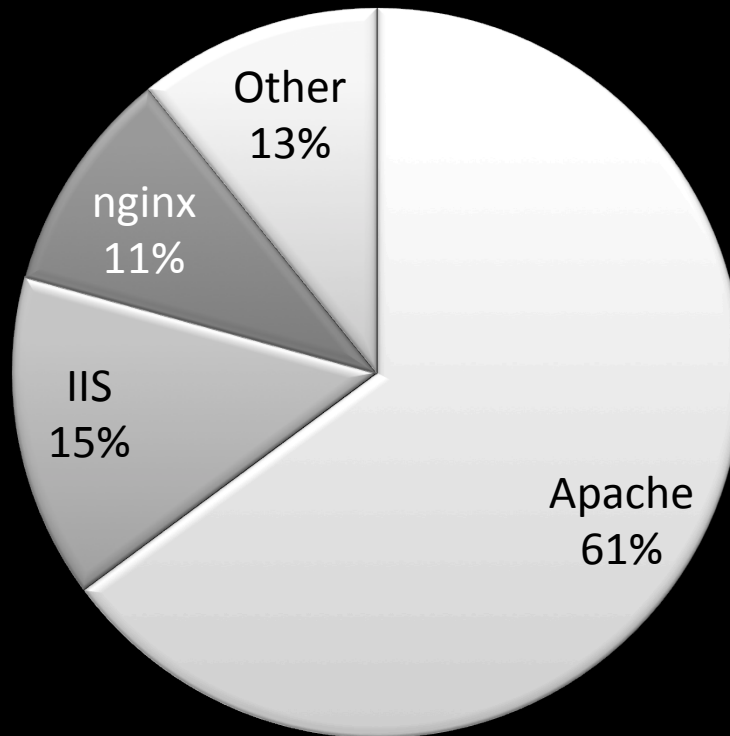
modsecurity
Open Source Web Application Firewall



blackhat
USA 2012

MODSECURITY: BEYOND APACHE

Web Server Platform Marketshare



Source: Netcraft: July 2012 Web Server Survey

One Config to Rule Them All



httpd.conf:
Include modsecurity.conf



web.config:
<Modsecurity enabled="true"
configFile="modsecurity.conf" />



nginx.conf:
ModSecurityConfig modsecurity.conf
ModSecurityEnable On

```
# Prevent path traversal (..) attacks
SecRule REQUEST_URI|ARGS "\.\.\/"
```

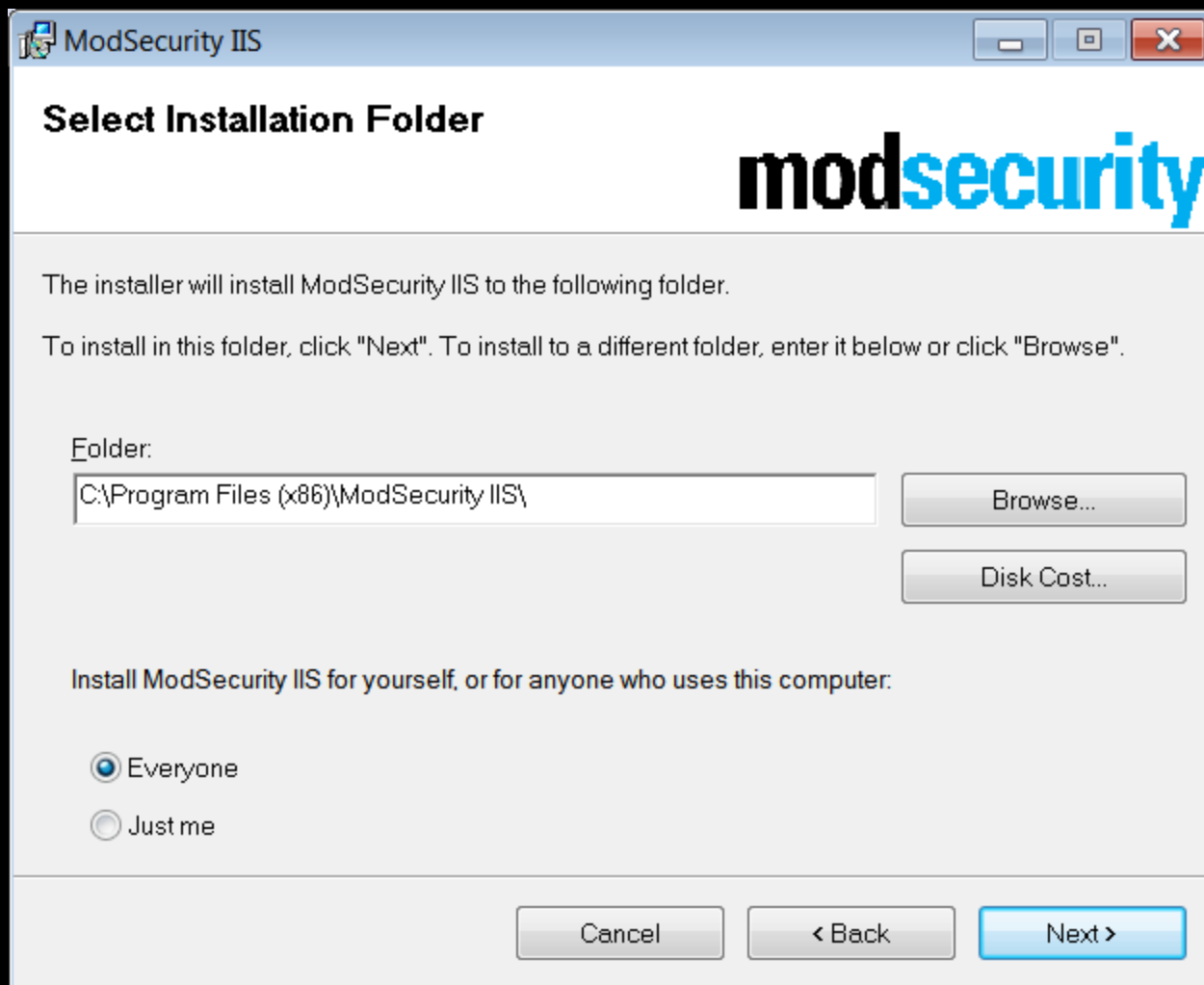
```
# Prevent XSS attacks (HTML/Javascript injection)
SecRule REQUEST_URI|ARGS "<(.\|\\n)+>"
```

```
# Very crude filters to prevent SQL injection attacks
SecRule REQUEST_URI|ARGS "delete[[:space:]]+from"
SecRule REQUEST_URI|ARGS "insert[[:space:]]+into"
SecRule REQUEST_URI|ARGS "select.+from"
```




blackhat
USA 2012

MODSECURITY IIS EXPERIENCE



ModSecurity IIS

License Agreement



Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

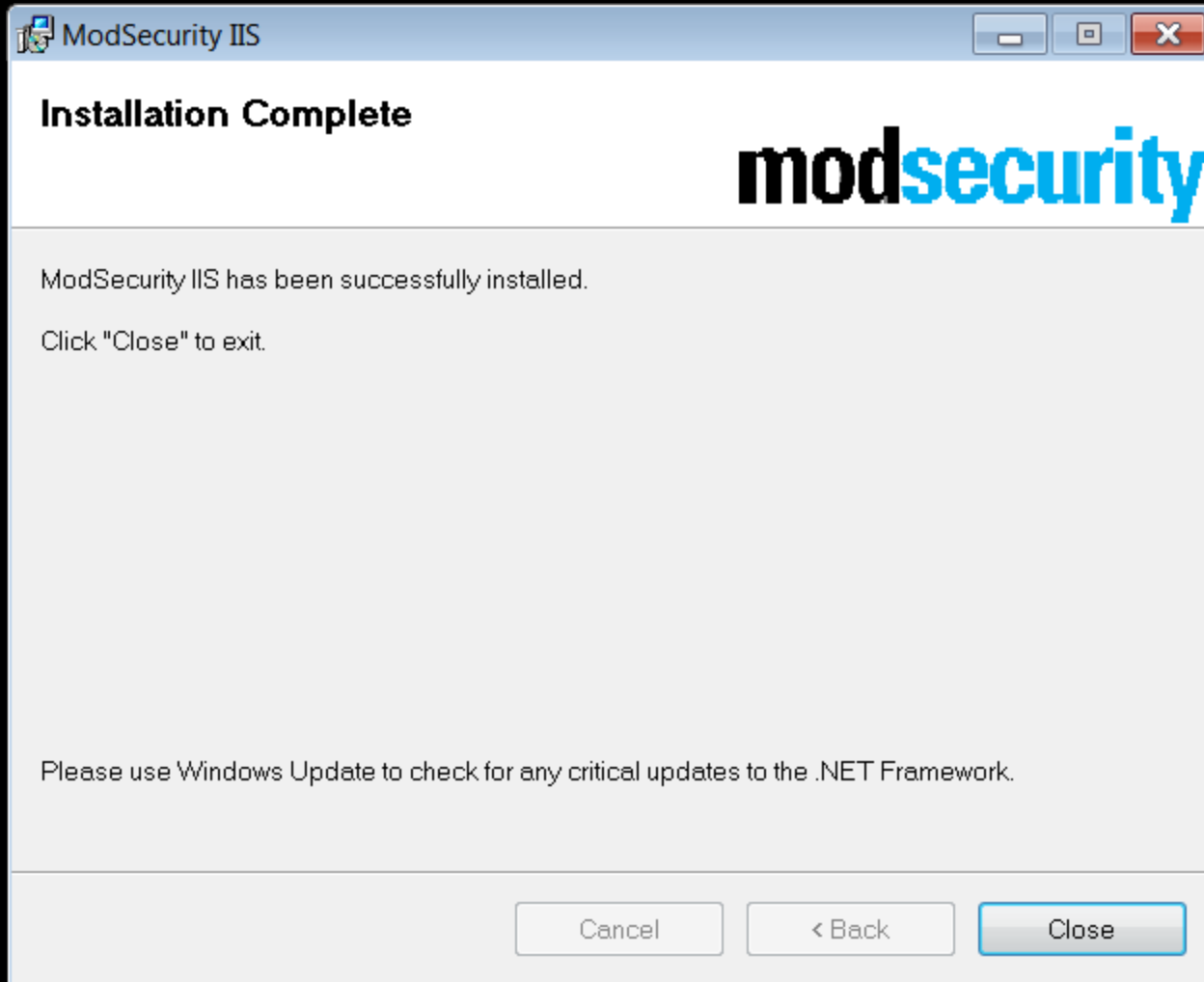
1. Definitions.

"License" shall mean the terms and conditions for use, reproduction...

☐ I Do Not Agree ☒ I Agree

Cancel < Back Next >







The image shows a Notepad window with the title bar 'Lister - [c:\inetpub\wwwroot\web.config]'. The menu bar includes 'File', 'Edit', 'Options', 'Encoding', and 'Help'. The status bar at the bottom right shows '100 %'. The text content is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <ModSecurity enabled="true" configFile="c:\inetpub\wwwroot\test.conf" />
  </system.webServer>
</configuration>
```

File View Help

Connections

- GREGS17 (gregs17\Gregs17)
- Application Pools
- Sites
 - Default Web Site
 - aspnet_client

 Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter:



Go



Show All

Group by:

Name	Status	.NET Framework	Managed by
ASP.NET v4.0	Start...	v4.0	Integrated
ASP.NET v4.0 Classic	Start...	v4.0	Classic
Classic .NET AppPool	Start...	v2.0	Classic
DefaultAppPool	Start...	v4.0	Integrated

- Add Application Pool...
- Set Application Pool Defaults...
- Start
- Stop
- Recycle...
- Basic Settings...
- Recycling...

Actions

- Add Application Pool...
- Set Application Pool Defaults...

Application Pool Tasks

- Start
- Stop
- Recycle...

Edit Application Pool

- Basic Settings...
- Recycling...
- Advanced Settings...
- Rename
- Remove
- View Applications
- Help

Ready

Event Properties - Event 0, ModSecurity

General Details

☒ Friendly ☐ XML View

+ System

- EventData

ModSecurity for IIS/2.7.0-rc2 (<http://www.modsecurity.org/>)
configured.

Copy

Close



blackhat
USA 2012

MODSECURITY NGINX EXPERIENCE

Build It

```
~/mod_security# ./configure
```

```
~/mod_security# cd standalone
```

```
~/mod_security/standalone# make
```

```
~/nginx-1.2.0# ./configure --add-  
module=../mod_security/nginx/  
modsecurity
```

```
~/nginx-1.2.0# make
```

```
~/nginx-1.2.0# make install
```

Debian - Windows Virtual PC

Action Tools Ctrl+Alt+Del

File: nginx.conf Line 38 Col 0 2803 bytes 45%

```
server_name localhost;

#charset koi8-r;

#access_log logs/host.access.log main;

location / {
    root html;
    index index.html index.htm;

    ModSecurityConfig /usr/local/nginx/conf/xss.conf;
    ModSecurityEnabled On;

#error_page 404 /404.html;

# redirect server error pages to the static page /50x.html
#
error_page 500 502 503 504 /50x.html;
location = /50x.html {
    root html;
}
```

1Help 2UnWrap 3Quit 4Hex 5Line 6 7Search 8Raw 9Format10Quit

Debian - Windows Virtual PC

ActionToolsCtrl+Alt+Del?

File: error.logLine 2 Col 08586 bytes18%

2012/06/26 01:41:29 [notice] 28716#0: nginx/1.2.0
2012/06/26 01:41:29 [notice] 28716#0: built by gcc 4.4.5 (Debian 4.4.5-8)
2012/06/26 01:41:29 [notice] 28716#0: OS: Linux 2.6.32-5-686
2012/06/26 01:41:29 [notice] 28716#0: getrlimit(RLIMIT_NOFILE): 1024:1024
2012/06/26 01:41:29 [notice] 28717#0: start worker processes
2012/06/26 01:41:29 [notice] 28717#0: start worker process 28718
2012/06/26 01:41:29 [info] 28718#0: ModSecurity for nginx/2.7.0-rc2 (http://www.modsecurity.org/) configured.
2012/06/26 01:41:29 [info] 28718#0: ModSecurity: APR compiled version="1.4.5"; loaded version="1.4.2"
2012/06/26 01:41:29 [info] 28718#0: ModSecurity: PCRE compiled version="8.30"; loaded version="8.30 2012-02-04"
2012/06/26 01:41:29 [info] 28718#0: ModSecurity: LIBXML compiled version="2.7.7"
2012/06/26 01:41:52 [info] 28718#0: *1 /test/index.html, client: 127.0.0.1, server: localhost, request: "GET /test/index.html HTTP/1.0", host: "127.0.0.1"
2012/06/26 01:41:52 [error] 28718#0: *1 open() "/usr/local/nginx/html/test/index.html" failed (2: No such file or directory), client: 127.0.0.1, server: localhost, request: "GET /test/index.html HTTP/1.0", host: "127.0.0.1"
2012/06/26 01:41:52 [info] 28718#0: *1 client 127.0.0.1 closed keepalive connection
2012/06/26 01:42:45 [info] 28718#0: *2 /test/ddd/../../../../index.html, client: 127.0.0.1, server: localhost, request: "GET /test/ddd/../../../../index.html HTTP/1.0"
2012/06/26 01:42:45 [info] 28718#0: [client 127.0.0.1] ModSecurity: Warning. Pat

1Help2UnWrap3Quit4Hex5Line67Search8Raw9Format10Quit



VIRTUAL PATCHING: EXAMPLES



CVE-2011-3414

Collisions in HashTable May Cause DoS Vulnerability

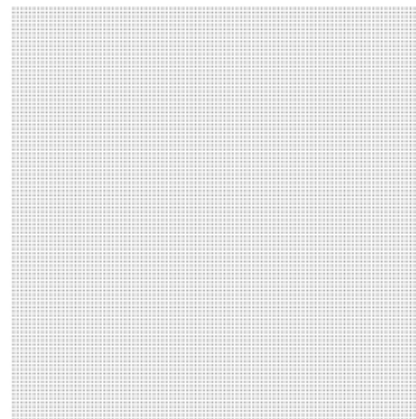
A denial of service vulnerability exists in the way that ASP.NET Framework handles specially crafted requests, causing a hash collision. An attacker who successfully exploited this vulnerability could send a small number of specially crafted requests to an ASP.NET server, causing performance to degrade significantly enough to cause a denial of service condition.

Lister - [d:\demo\payload]

File Edit Options Encoding Help 0 %

3QBZJK5ZX=&NEUQ7BWAU6=&6902D0YP6J=&9PZGHCDJYD=&NU73S3KNU=&IF686YJQJ8K=&9XUU
CJEENJ=&FX4A75F91FM=&IGJKQVBZAVK=&LJUJU6J3UZ=&X7GJ5MWWY=&6AVIZWTUK=&WQNIQ70
ZMS=&IM1UKMZHK6F=&D09WX2R9H=&RYLZSIQT8U=&KR9BBFUH2E=&UI8N4SWUWW=&TL5F6URUPP
=&B1P81FWDSUU=&CM6Y80XSA0=&LE72GBPWB=&EEFMULEXC=&M6FKM13WB=&MGN8123XA2K=&ZM
I35GXHMN=&LXQQOM138LL=&XXST36DRX=&JRYRU54TFZ=&LGG3X9MFN7=&MH1NI402I22=&MHFI
KIM0TEH=&BWPRUCQ4X3=&RM6K7U75WZ=&SMIAE6PAL4=&MOCGW14ZU7=&I0JKKKOG7EN=&Q4B9U
7L3UZ=&23UAYU5B31=&9TRJE0XRWQ=&3Q3LKPC2K0=&D3ACY8973E=&UGJPMCQHP=&AU6THWSCA
7=&MH5SM8NPWB1=&P57KEP668X=&81C4LQ4DFY=&MPJBASYMRM=&25EWGNN5NE=&R1FFQRM5T=&
28HUK0QHY=&HQN8TCEF80=&XNXKKGA26=&HGKBTESRZ=&JRF6S5UDTD=&38LYMK6E25=&LWJ9ZP
MJBK=&MIIPJFF9IQZ=&T7NR6K1WH=&320X9ZI2EG=&6XOUR0M63Q=&Q30KI9EPH8=&MIH8YKJQ1
GG=&N3E5JY88DU=&61CFH01CK0=&MJJ0BGBNFLR=&0WWGKU5U41=&6BALUUUD70=&WP8RSB0FOI
=&LXS45ETZC4U=&0ZPQL9FA5=&1XTRHULNN1=&8CM190RQRL=&30AY630K3E=&G6REPF004H=&3
J3D3UNH0N=&BZQFCAP6FDE=&MTHW3ALU7U=&2JS320Y101=&B0YC5TXNB1=&LNOJU48BS=&D07Z
A81NOJU=&Y5NYWOTNBW=&L1EQYKFQ66=&GQQK1DW76C=&CQ29SZT9Q=&4GR6HUU473=&YGYUZBX
20=&DD8CT8BIP=&H1YT271ZWA=&JJBUT364HU=&NBQI03HG4=&AUOCATLKQ4=&CUXC3C6EX9=&8
B0DP2W00H=&LD0JAGD783=&IE8Z8920XU0=&IU8BODMF93=&J5NU4WRJ3=&KSL8ADCBBS5=&PX4
Q06YCEX=&5AC6J6ZNE=&NPRUWDUVOBH=&T9J3LGT57E=&BJPHHFU5R=&UP06A0G7ZH=&2KNAKSU
PP4=&U56TPL0PLB=&ZS7GXLL58=&CDJSSBGKHG=&BZOT9HXJU60=&NP37RNJXEMP=&I9GBUL4Z7
HR=&UIXSRTUTK4=&KJIW62MYC=&FPIWCZFJ1=<LGE0EI9=&NA0KPUB6SZ=&KM9XU9HHD=&9RM
F3TN20G=&1BAHABFZMD=&9W25U41EF6=&IUVDHERY3T=&A0YWSYUHP=&1ZCUQK1SYP=&5Q0BSC
ERW5=&U0T80SU5KN=&DQ5PMITM67=&QGA2WU0N6=&1WT1LRSW5=&QBLIU6KE7=&2RTX2E40J9=&
YJ20S0ZJBL=&FU10MSK77T=&4NP7K9A2WG=&IEW7806CQQB=&713BE9XHBU=&WQDLRNYUYUK=&UP
UDDWCD06=&8DSWBN8E27C=&8SMOTNCK200=&8W0URSCUE0T=&8FK6827E0C=&8T1TE00E7UD=&8D22UT7

ASP.NET: effectiveness



1 dot $\approx$ 3 CPU cores

1 Gbit/s $\rightarrow$ keep $\sim$ 30k Core2 cores busy



Mitigations

- Restrict the request body size
 - Restrict the number of ARGS
 - Identify repetitive payloads
 - Check ARGS names against PoC data
- ✓ There are ModSecurity rules for all four mitigations

```
Listner - [c:\inetpub\wwwroot\test.conf]
File Edit Options Encoding Help 100 %

SecAuditLogStorageDir c:\temp

# The index of all files created
# YOU MUST NOT ALLOW NON-ROOT USERS TO WRITE
# TO THE BASE FOLDER
SecAuditLog c:\temp\index

# Choose what to log ■ everything (default is ABCFHZ)
SecAuditLogParts ABCDEFGHZ

SecAuditEngine On

SecRule &ARGS "@ge 1000" "chain,id:1234,phase:2,t:none,deny,msg:'Possible Hash DoS Atta
    SecRule REQUEST_BODY "^\w*?=(.*?)&\w*?=(.*?)&\w*?=(.*?)&\w*?=(.*?)&" "chain,cap
        SecRule TX:1 "@streq %{tx.2}" "chain,setvar:tx.hash_dos_match=+1"
            SecRule TX:2 "@streq %{tx.3}" "chain,setvar:tx.hash_dos_match=+
                SecRule TX:3 "@streq %{tx.4}" "chain,setvar:tx.hash_dos
                    SecRule TX:HASH_DOS_MATCH "@eq 3"

#SecRule ARGS_NAMES "@pmFromFile hash_dos_param_names.txt" "phase:2,t:none,block,msg:'h
```

Event Properties - Event 0, ModSecurity

General Details

☒ Friendly ☐ XML View

+ System

- EventData

[client 127.0.0.1] ModSecurity: Access denied with code 403 (phase 2).
Operator EQ matched 3 at TX:hash_dos_match. [file
"c:\inetpub\wwwroot\test.conf"] [line "41"] [id "1234"] [msg "Possible
Hash DoS Attack Identified."] [tag
"http://blogs.technet.com/b/srd/archive/2011/12/27/more-
information-about-the-december-2011-asp-net-vulnerability.aspx?
Redirected=true"] [hostname "GREGS17"] [uri "/default.htm"]
[unique_id "18302628887781180653"]

Copy

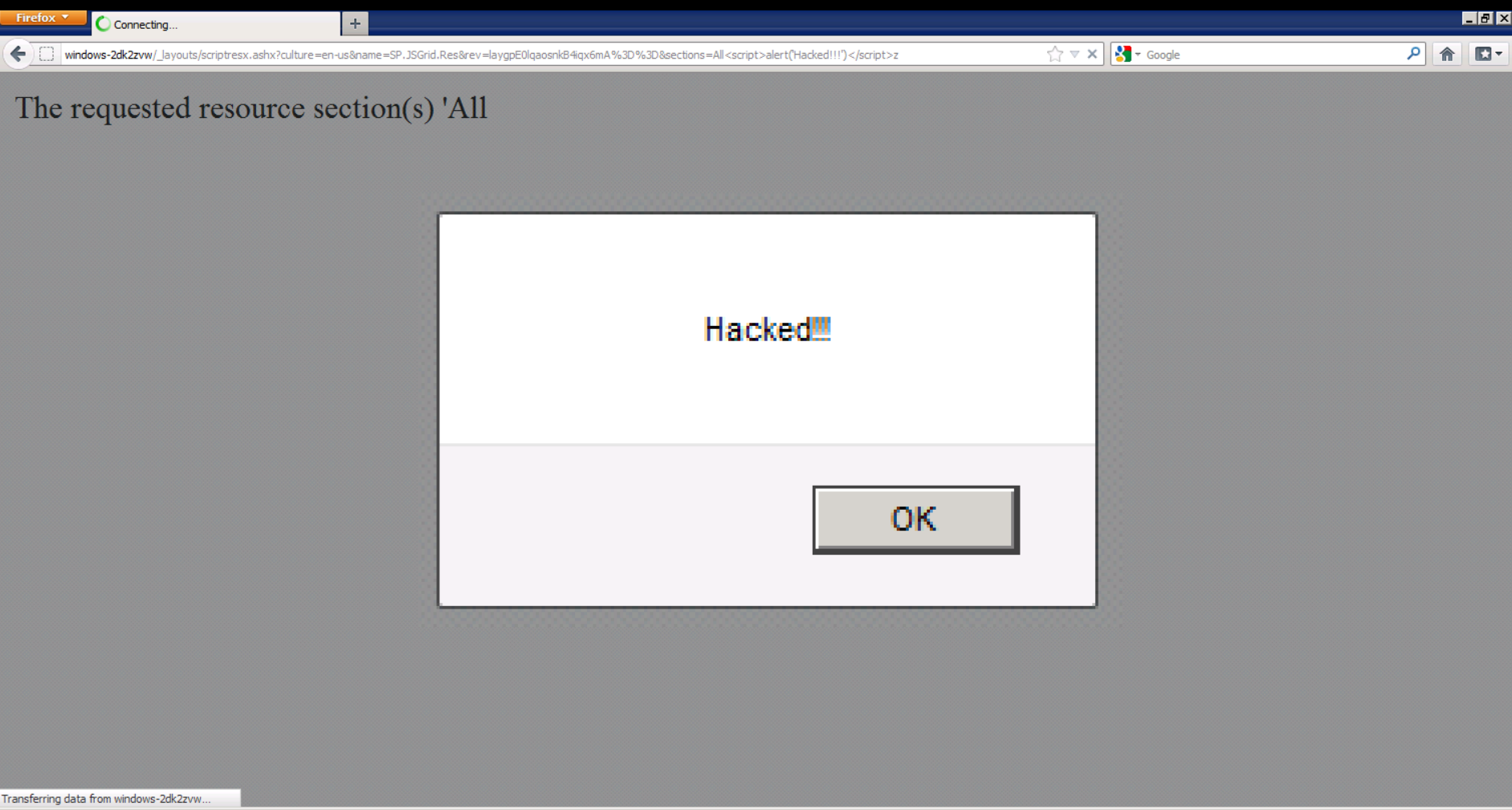
Close

CVE-2012-1859

- A classic case of cross-site scripting vulnerability

http://sharepoint/_layouts/scriptresx.ashx?culture=en-us&name=SP.JSGrid.Res&rev=laygpE0lqaosnkB4iqx6mA%3D

[**<SCRIPT>ALERT\('HACKED!!!'\)</SCRIPT>z**](http://sharepoint/_layouts/scriptresx.ashx?culture=en-us&name=SP.JSGrid.Res&rev=laygpE0lqaosnkB4iqx6mA%3D§ions=All)





OH SHIT
THERES NO ESCAPE

CVE-2012-1859

- Blacklist approach:

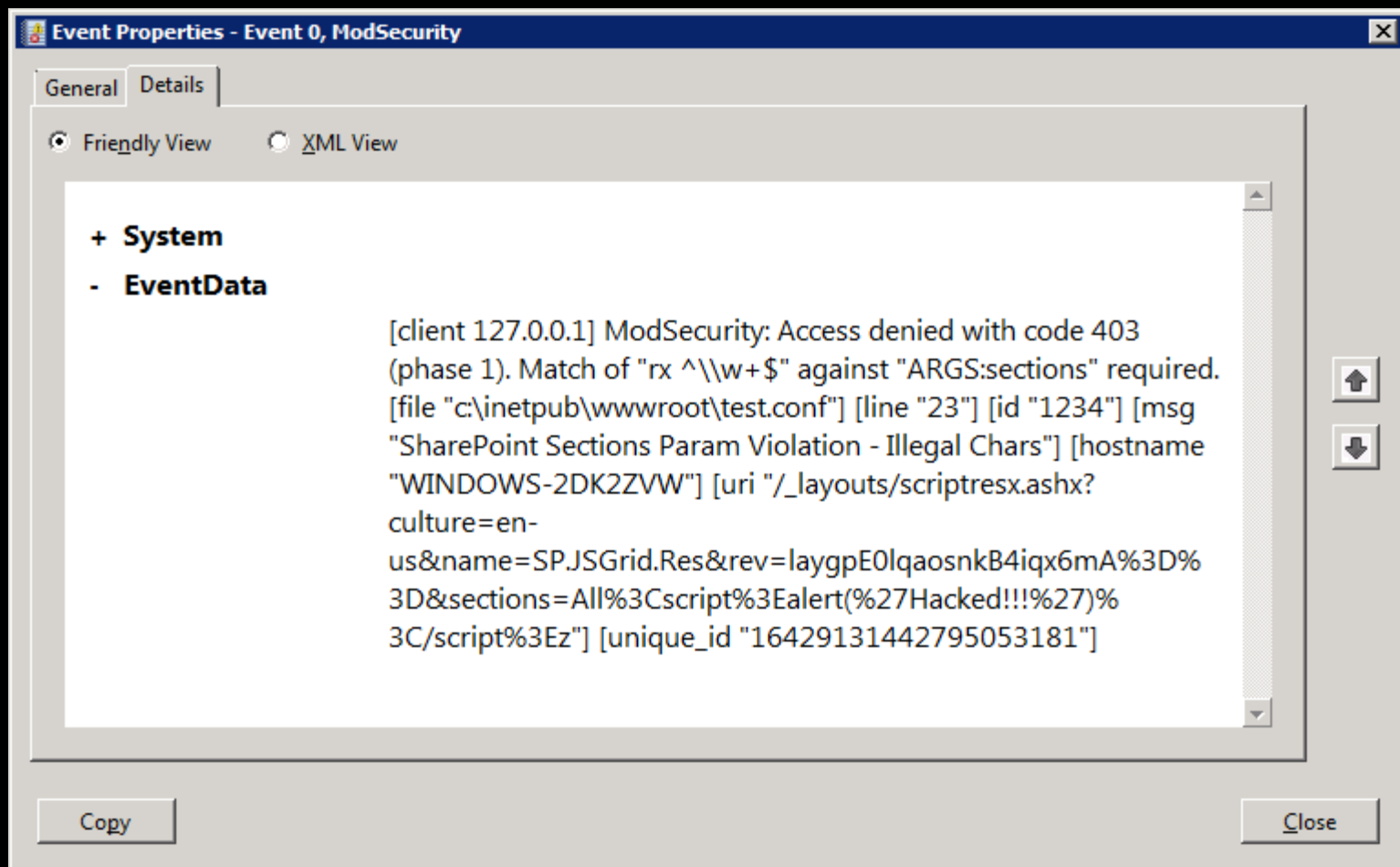
```
SecRule REQUEST_FILENAME "@contains /_layouts/  
scriptresx.ashx" "chain,phase:1,block,msg:'XSS  
Attempt Against SharePoint"
```

```
SecRule ARGS:sections "@pm < > ( ) ; :"
```

- Whitelist approach:

```
SecRule REQUEST_FILENAME "@contains /_layouts/  
scriptresx.ashx" "chain,phase:1,block,msg:'SharePoint  
Sections Param Violation - Illegal Chars"
```

```
SecRule ARGS:sections "!@rx ^\w+$"
```





MODSECURITY 2.7.0: FIRST MULTI-PLATFORM RELEASE

Download RC2 Now

- <http://sourceforge.net/projects/modsecurity/files/modsecurity-apache/2.7.0-rc2/>
- http://sourceforge.net/projects/modsecurity/files/modsecurity-iis/2.7.0-rc2/ModSecurityIIS_2.7.0-rc2.msi

New Protections Coming

- Microsoft Security Response Center will start publishing ModSecurity rules for vulnerabilities in Microsoft products
- IIS/ASP/ASP.NET specific ModSecurity rule sets will be created by community effort



blackhat
USA 2012

SUMMARY

Resources

- ModSecurity home page
 - <http://www.modsecurity.org/>
- OWASP Core Rule Set for ModSecurity
 - https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project
- MSRC blog
 - <http://blogs.technet.com/b/srd/>
- Trustwave SpiderLabs blog
 - <http://blog.spiderlabs.com/>
- Trustwave Commercial Rule Set for ModSecurity
 - <https://www.trustwave.com/modsecurity-rules-support.php>

Contributors

- Microsoft – ModSecurity Port for IIS
 - Greg Wroblewski – Senior Security Developer
 - Suha Can – Security Researcher / Developer
- Trustwave - ModSecurity
 - Ziv Mador – Director of Security Research
 - Ryan Barnett – Security Researcher Lead
 - Breno Pinto – ModSecurity Researcher & Developer
- Open community - Security Port for Nginx
 - Alan Silva - Software Engineer at Alcatel-Lucent



BLACK HAT ARSENAL SESSIONS

WEDNESDAY, 3:30PM, POD 2

THURSDAY, 10:15AM, POD 2



blackhat
USA 2012

**THANK YOU
FEEDBACK:
RBARNETT@MODSECURITY.ORG**