ModSecurity as Universal Cross-platform Web Protection Tool

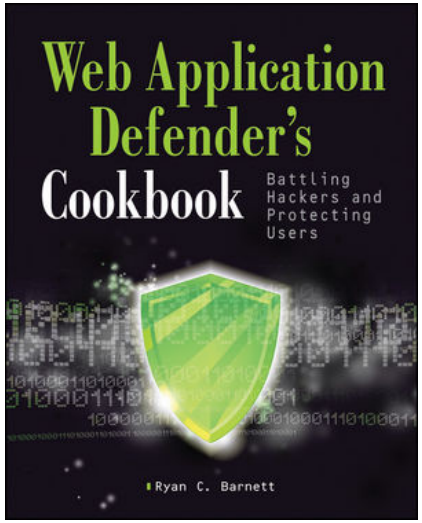
Ryan Barnett
Greg Wroblewski

Trustwave® SpiderLabs®

modsecurity

Open Source Web Application Firewall

OWASP



Web Application Security Consortium

black hat® USA 2012


Port Scan
ALPHA ZONE
BETA ZONE
North Sloberia
Strategic Zero Day Reserve
Valley of the Worms
Zorkuldonia
(new capital)
Root Kit Pass
KLUGES REGION
Sploit Market
East Sloberia
Geekland
HACKISTAN
Fuzz Forest
HIGH MEMORY REGION
Patch Delta
Buffervilla
(former capital)
Malvaria
Bugburg
UPPER 01
Phrack Training Camp
Breach Valley
Sea Plus Plus
LOWER 01
Freedonia

InPrivate http://blogs.technet.com/b/srd/about.aspx About Security Rese...

Microsoft

Security Research & Defense

Information from Microsoft about vulnerabilities, mitigations and workarounds, active attacks, security research, tools and guidan

TechNet Blogs > Security Research & Defense > About Security Research & Defense

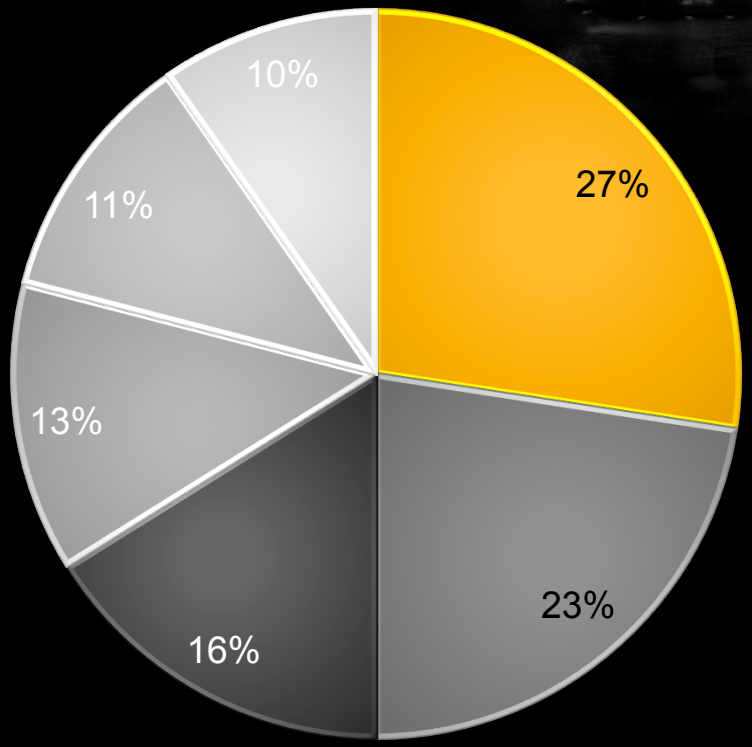
Options

InPrivate http://blogs.technet.com/b/srd/about.aspx About Security Rese...

Greg Wroblewski Bio: Greg Wroblewski, Senior Security Software Engineer, drives technical side of the security response process at Microsoft. His experience at breaking things started at the age of three, when he successfully broke a power outlet. Surviving this achievement he decided to move his attention towards low voltage devices. Guided by his parents, he eventually settled on software breaking and protecting techniques. Currently as a member of the MSRC Engineering team he is well known for always keeping his development environment updated with newest malware available. Since the time of the WMF vulnerability outbreak, he now keeps his office equipped with a reasonable amount of water, MREs and fire logs. Always prepared to keep customers secure.

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

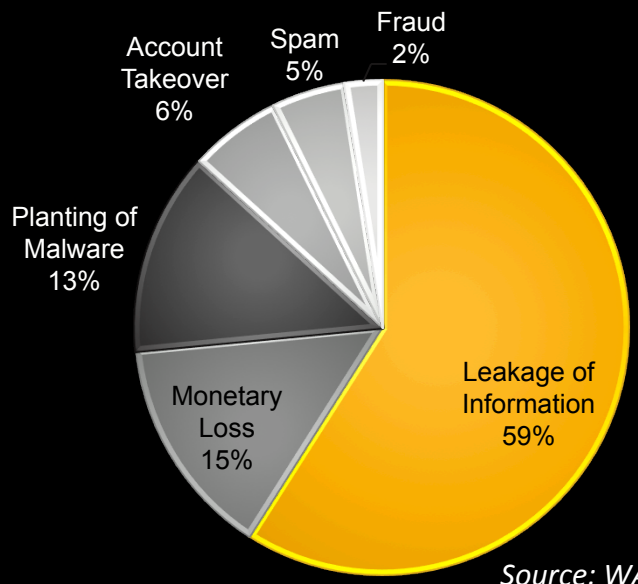
.....Wait for it.....

WHID
Web Hacking Incident Database

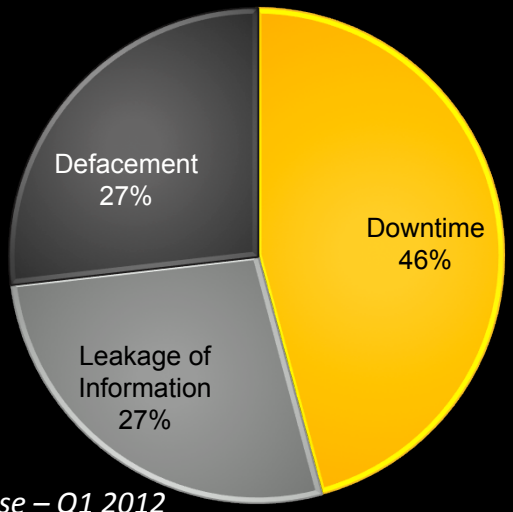
Hackers Breach Credit Card Processor; 50K Cards Compromised

CIA site downed as Anonymous claims attack

Profit



Hacktivism

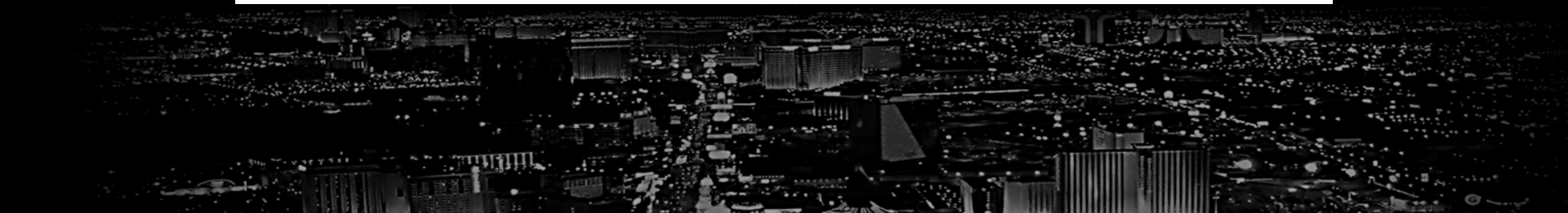


Source: WASC Web Hacking Incident Database – Q1 2012

WHY MODSECURITY?

Virtual Patching Definition:

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



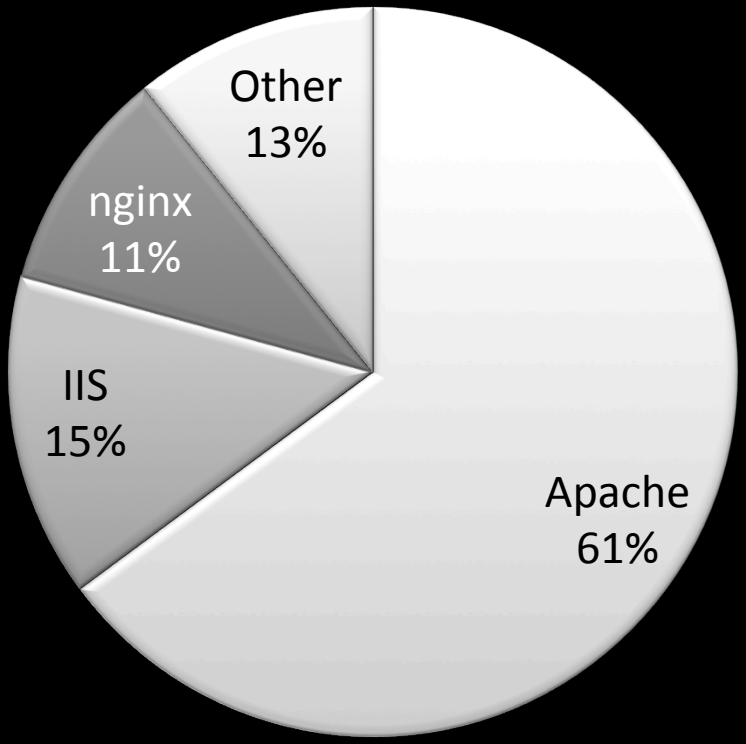
ModSecurity as Virtual Patching Tool

- 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: BEYOND APACHE

Web Server Platform Marketshare



Source: Netcraft: July 2012 Web Server Survey

One Config to Rule Them All

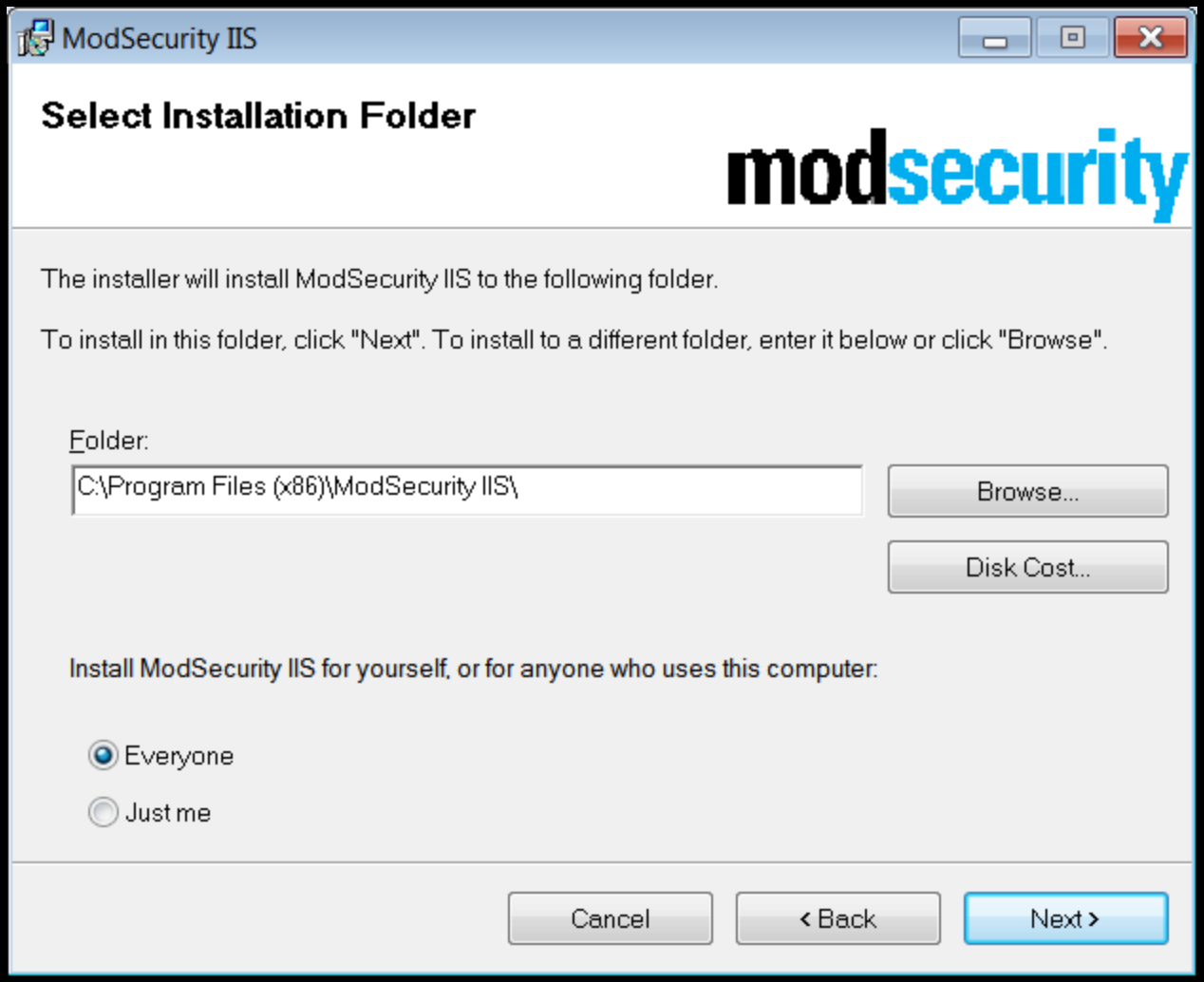

```
httpd.conf:
Include modsecurity.conf
```

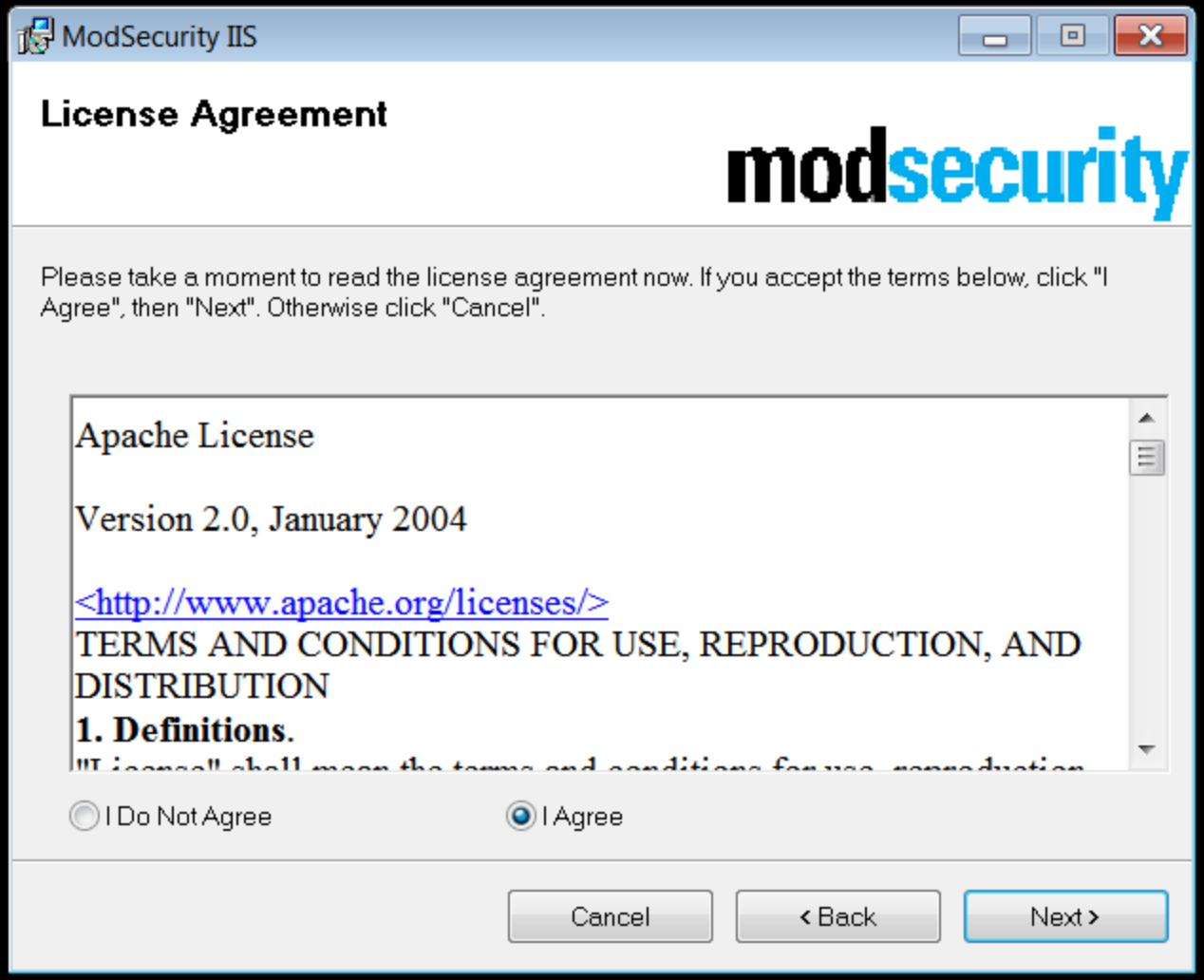

```
web.config:
<Modsecurity enabled="true"
configFile="modsecurity.conf" />
```

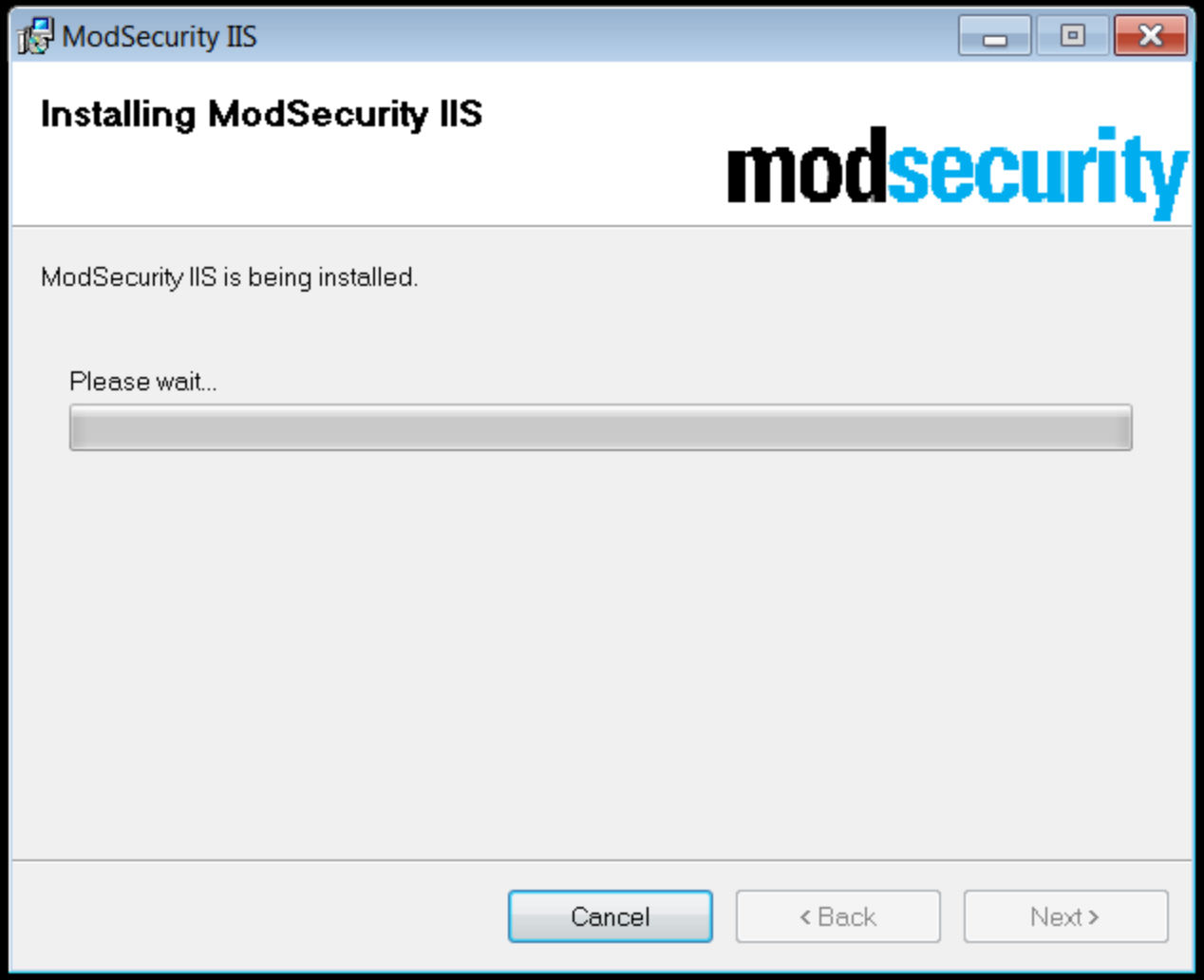

```
nginx.conf:
ModSecurityConfig modsecurity.conf
ModSecurityEnable On
```

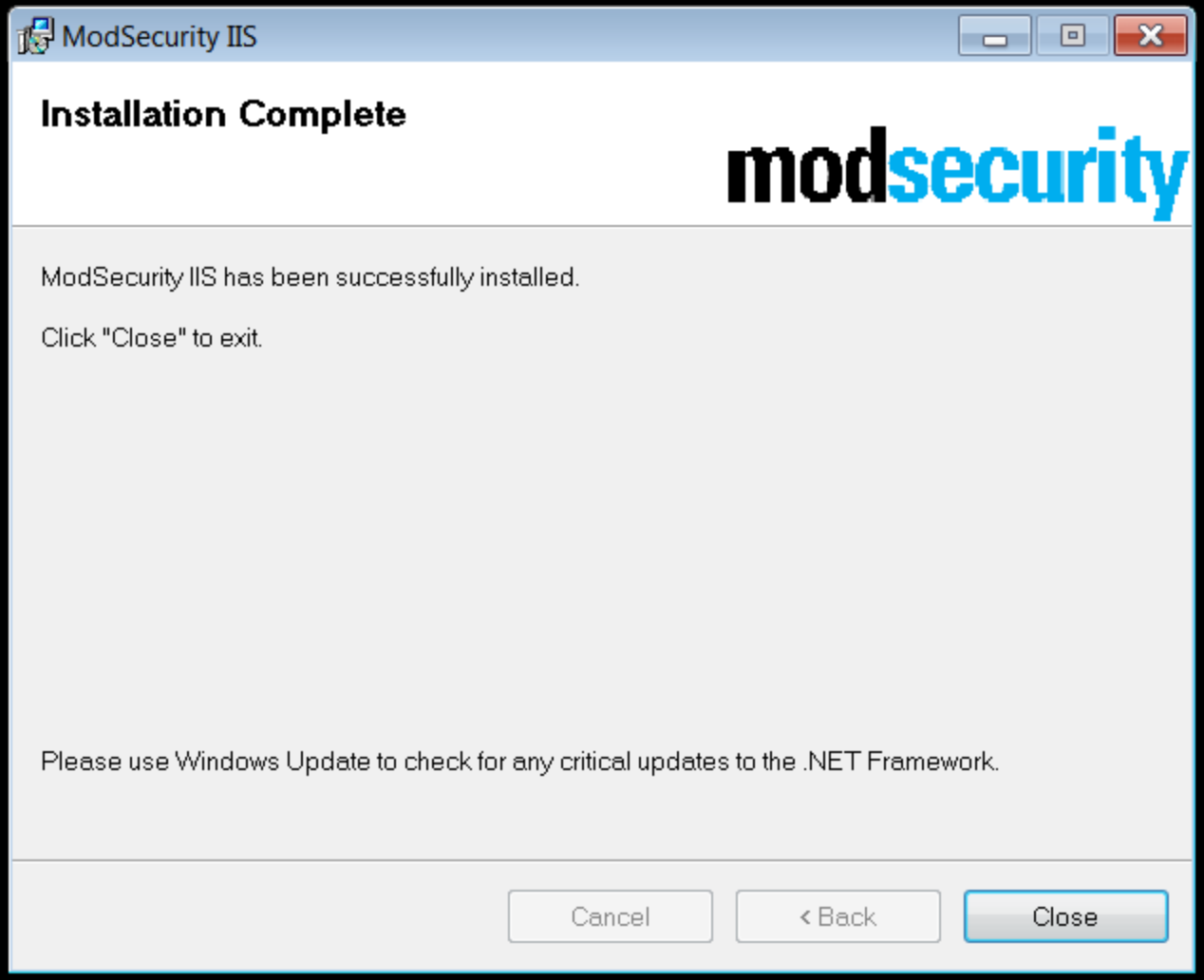
```
# Prevent path traversal (..) attacks
SecRule REQUEST_URI|ARGS "\.\./"

# Prevent XSS atacks (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"
```

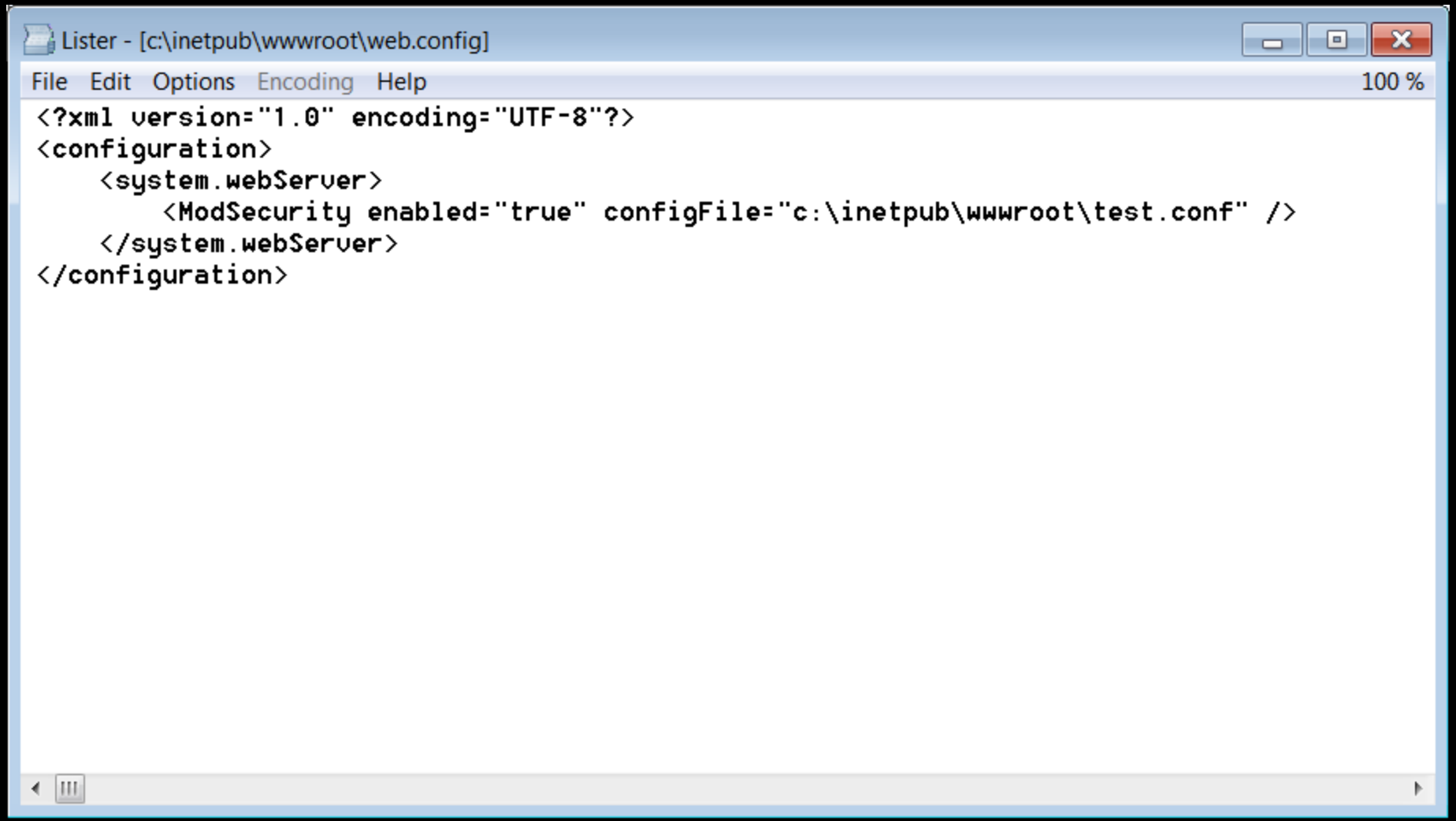
MODSECURITY IIS EXPERIENCE

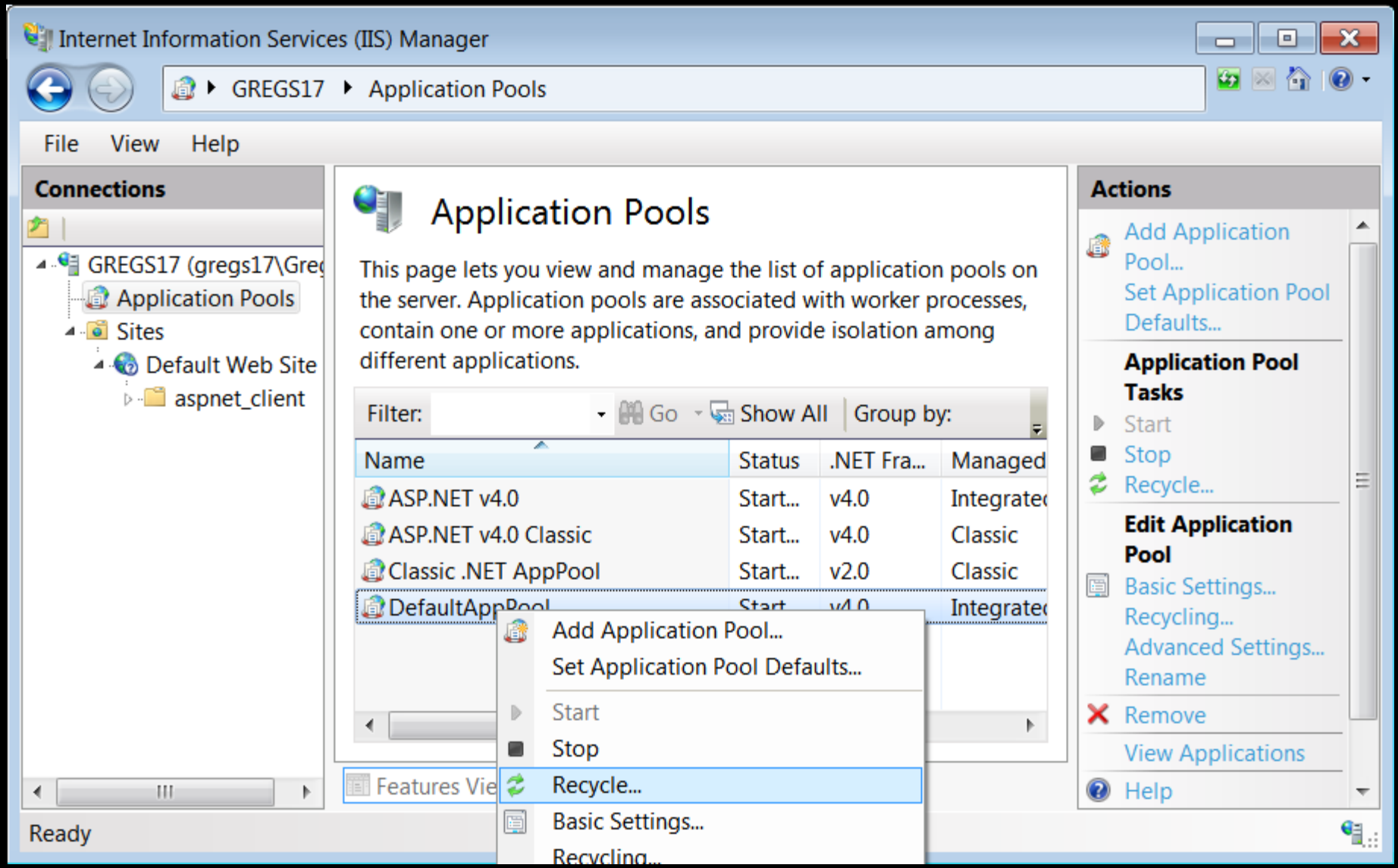


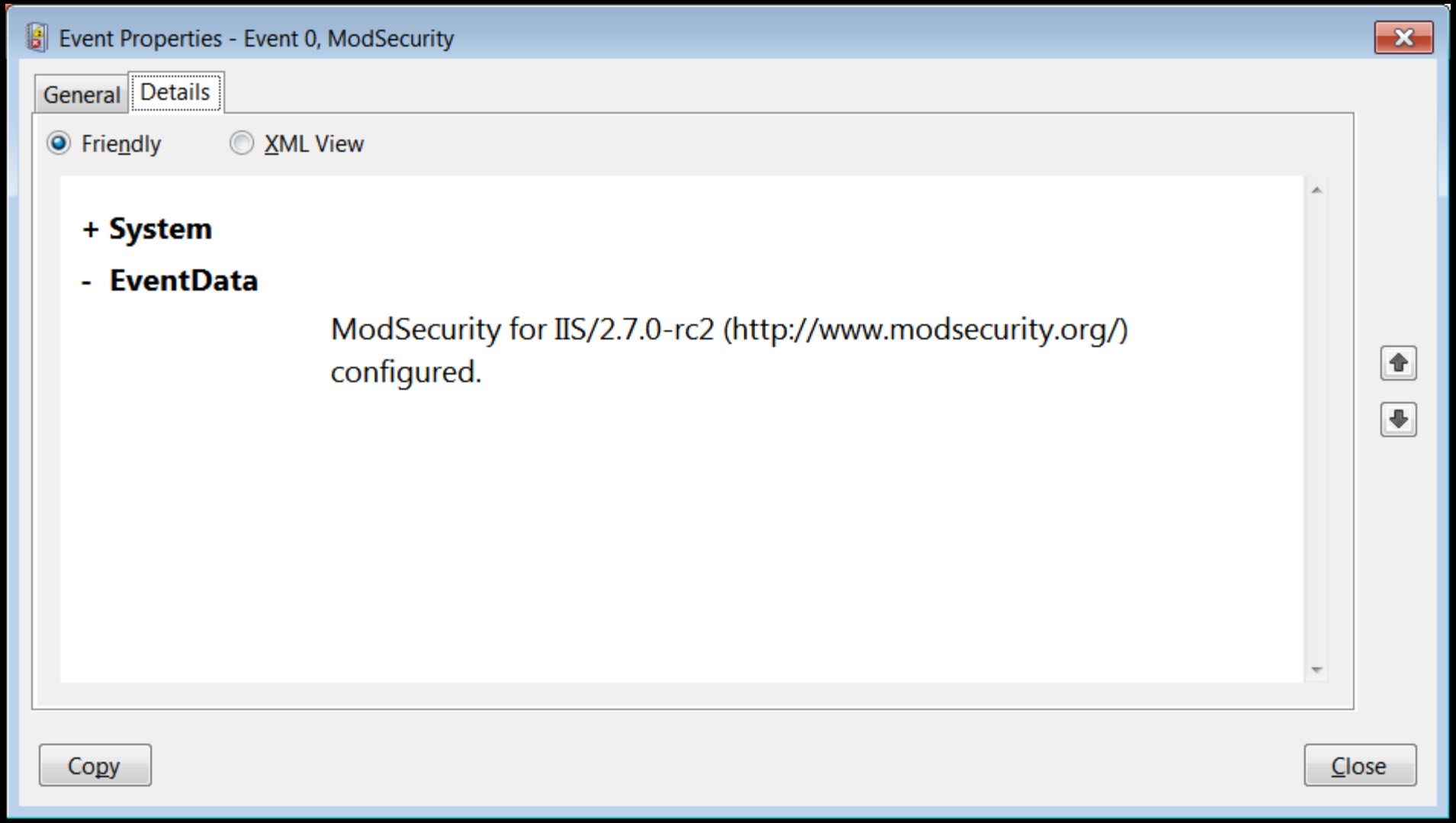








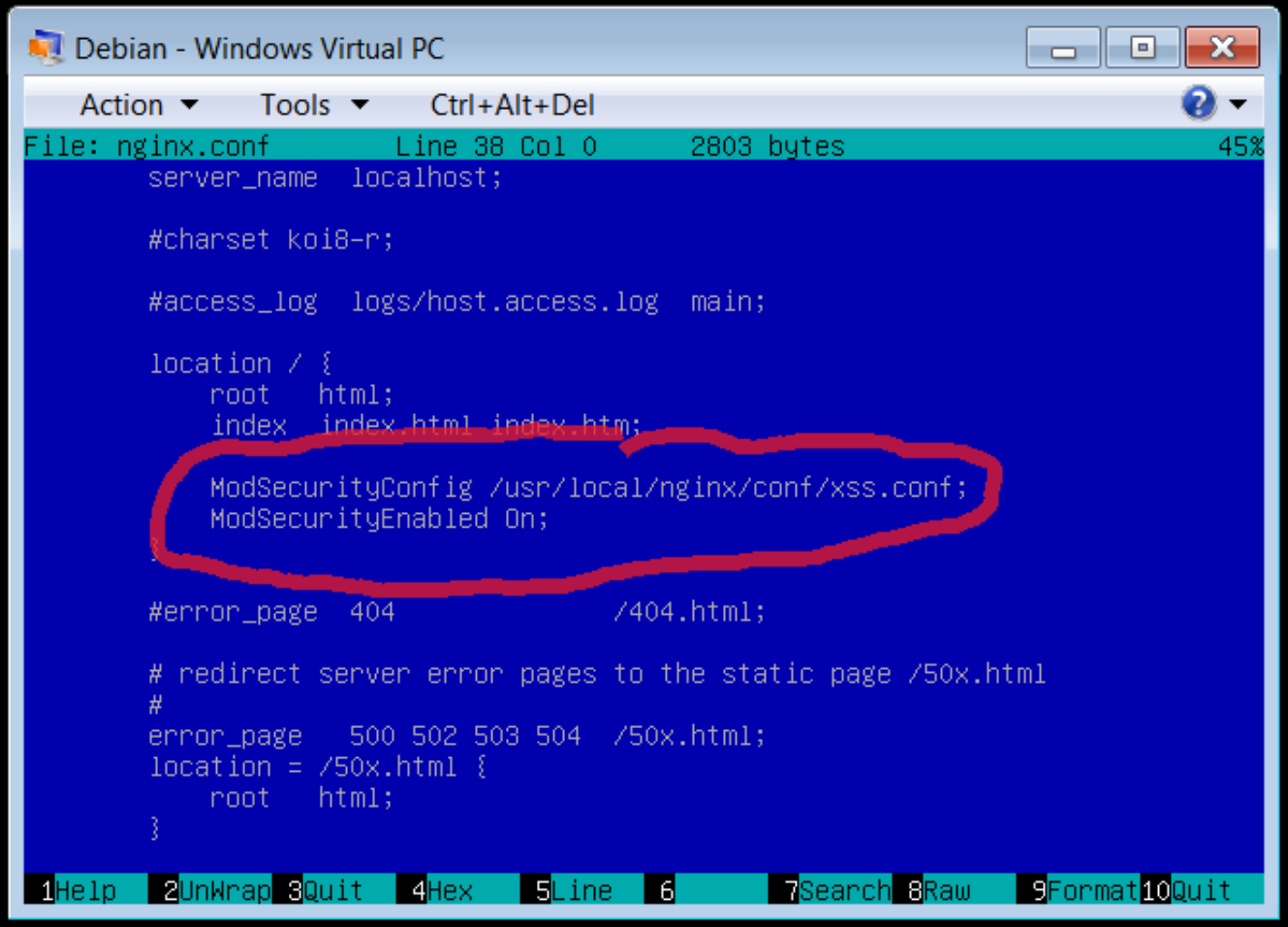


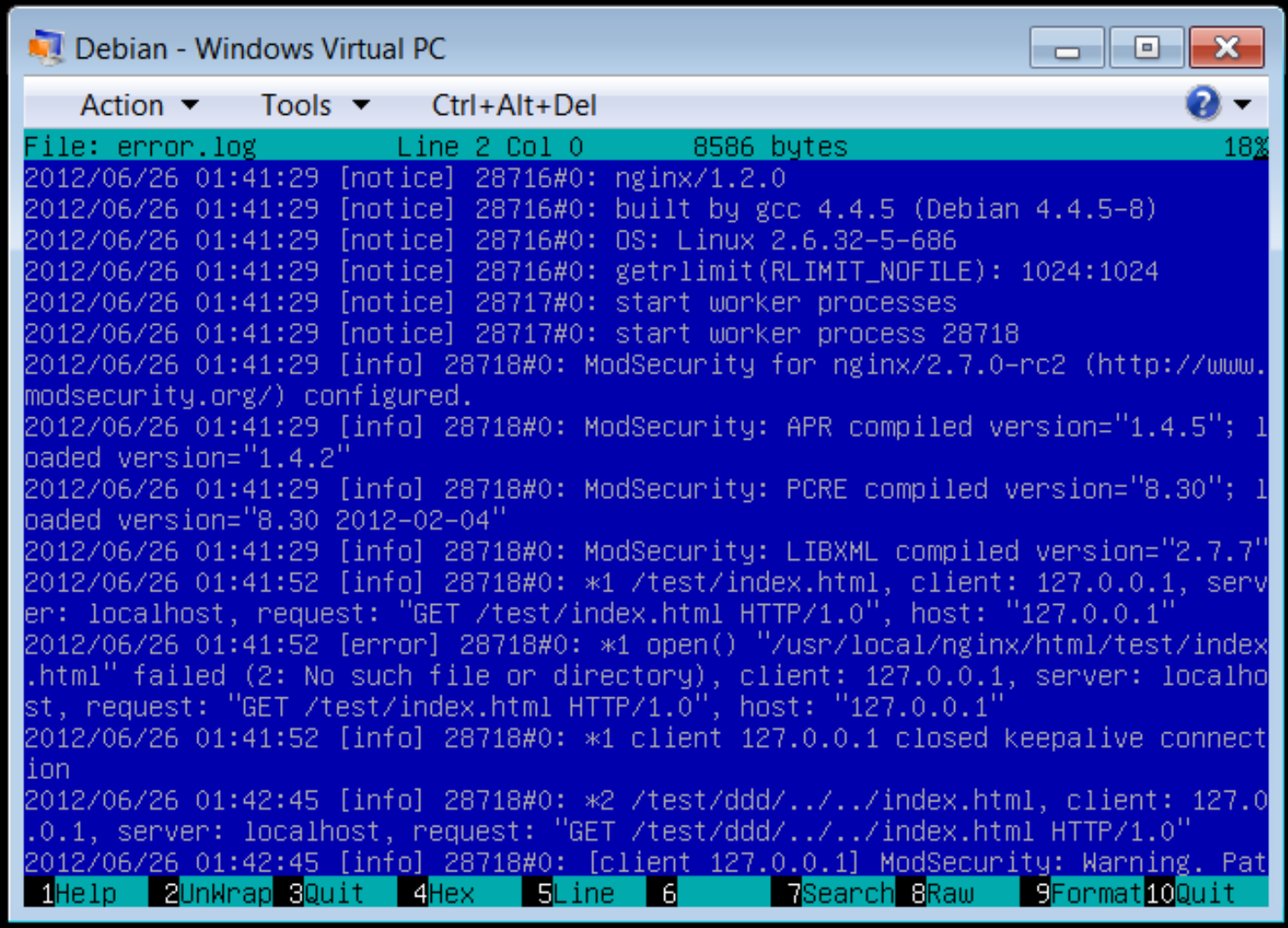


MODSECURITY NGINX EXPERIENCE

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
```



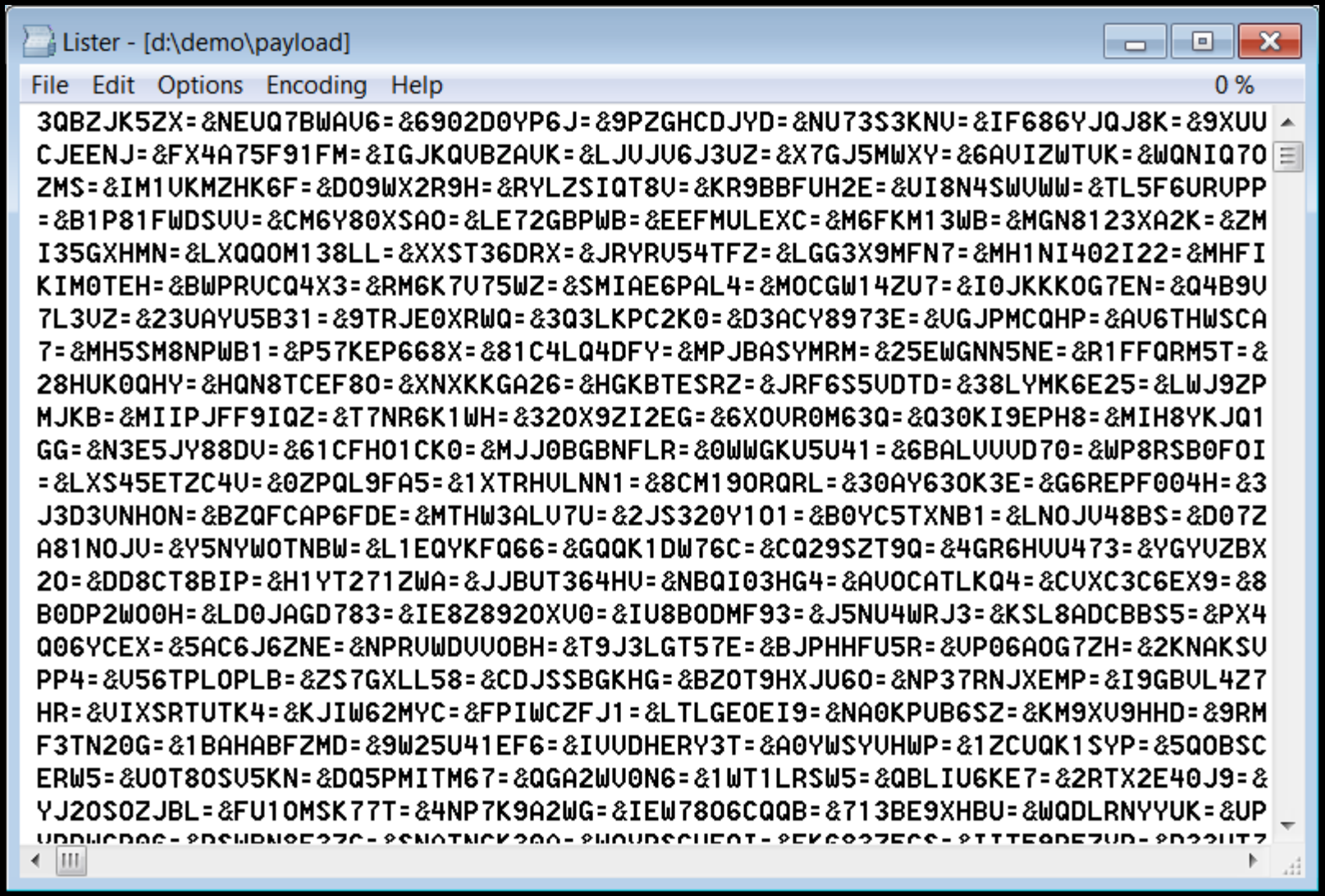


VIRTUAL PATCHING: EXAMPLES

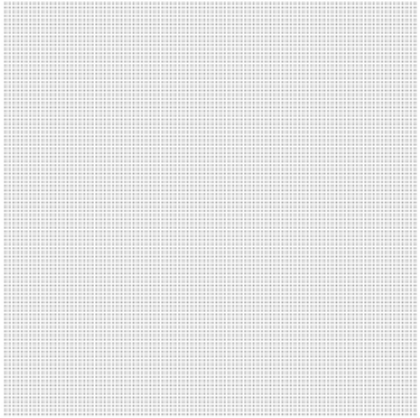
CVE-2011-3414

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.



ASP.NET: effectiveness



1 dot ≈ 3 CPU cores

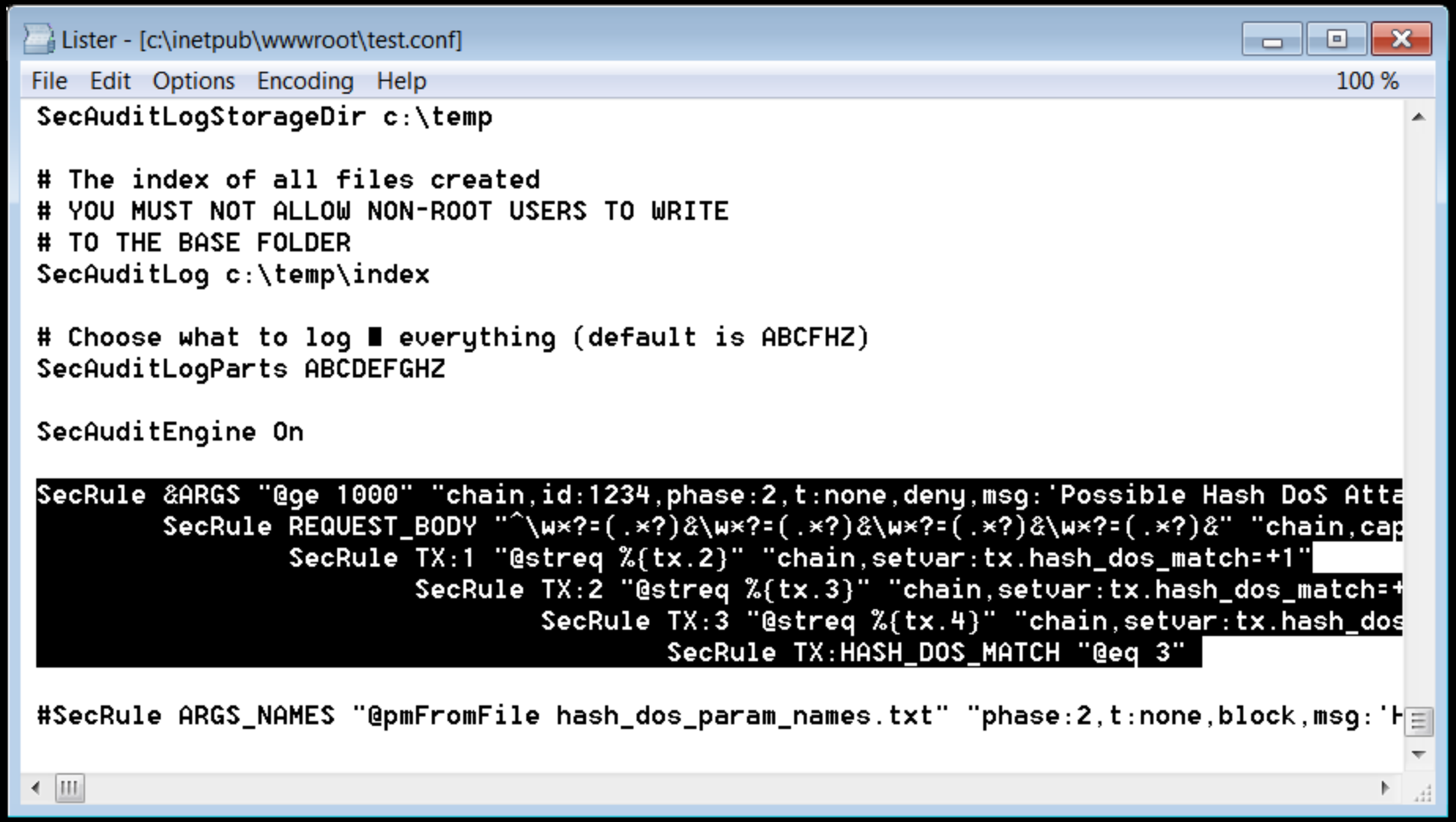
1 Gbit/s → keep ~30k Core2 cores busy

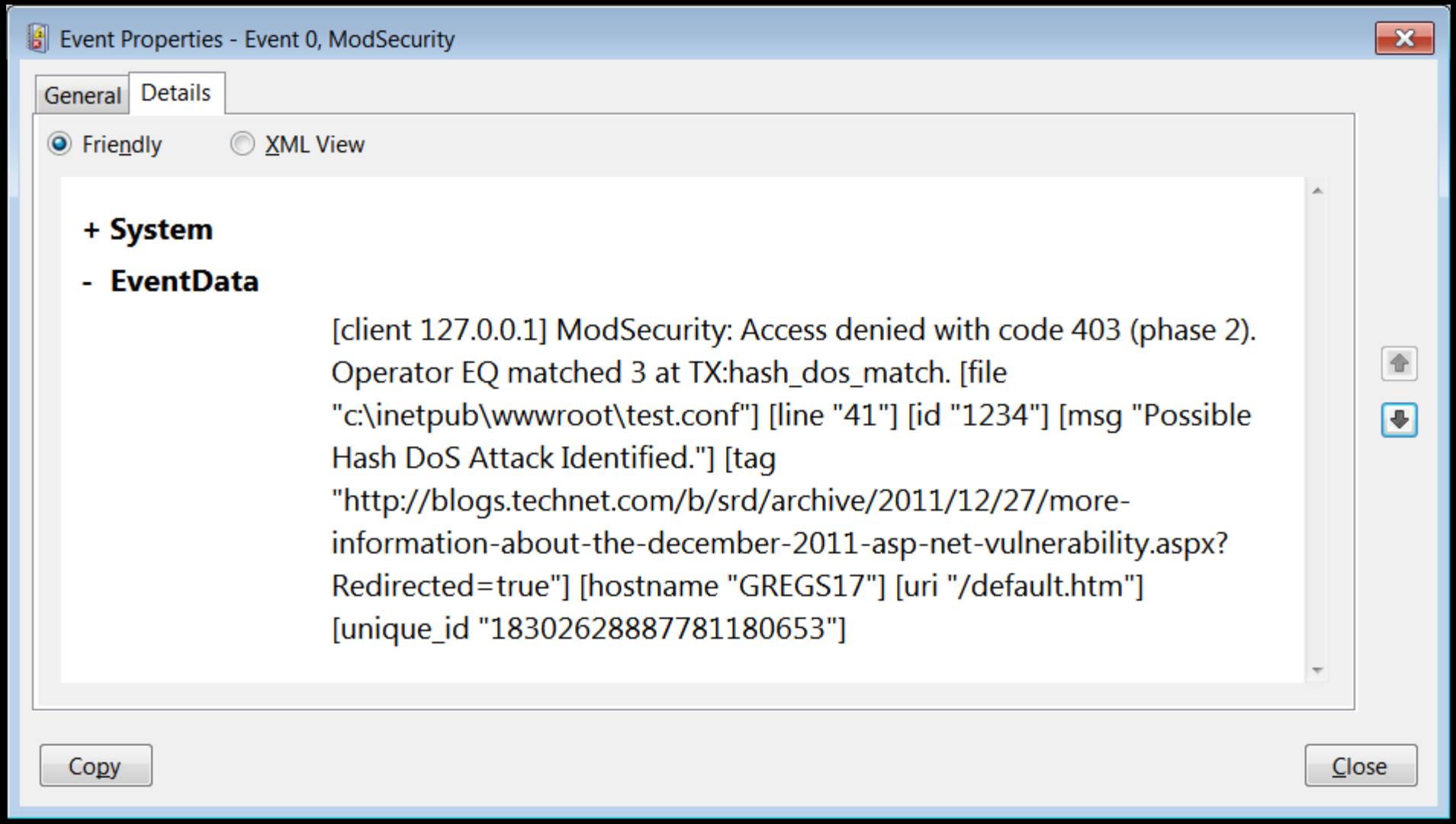

RESTROOM CLOSED
NO ENTRY
化粧室
使用禁止

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

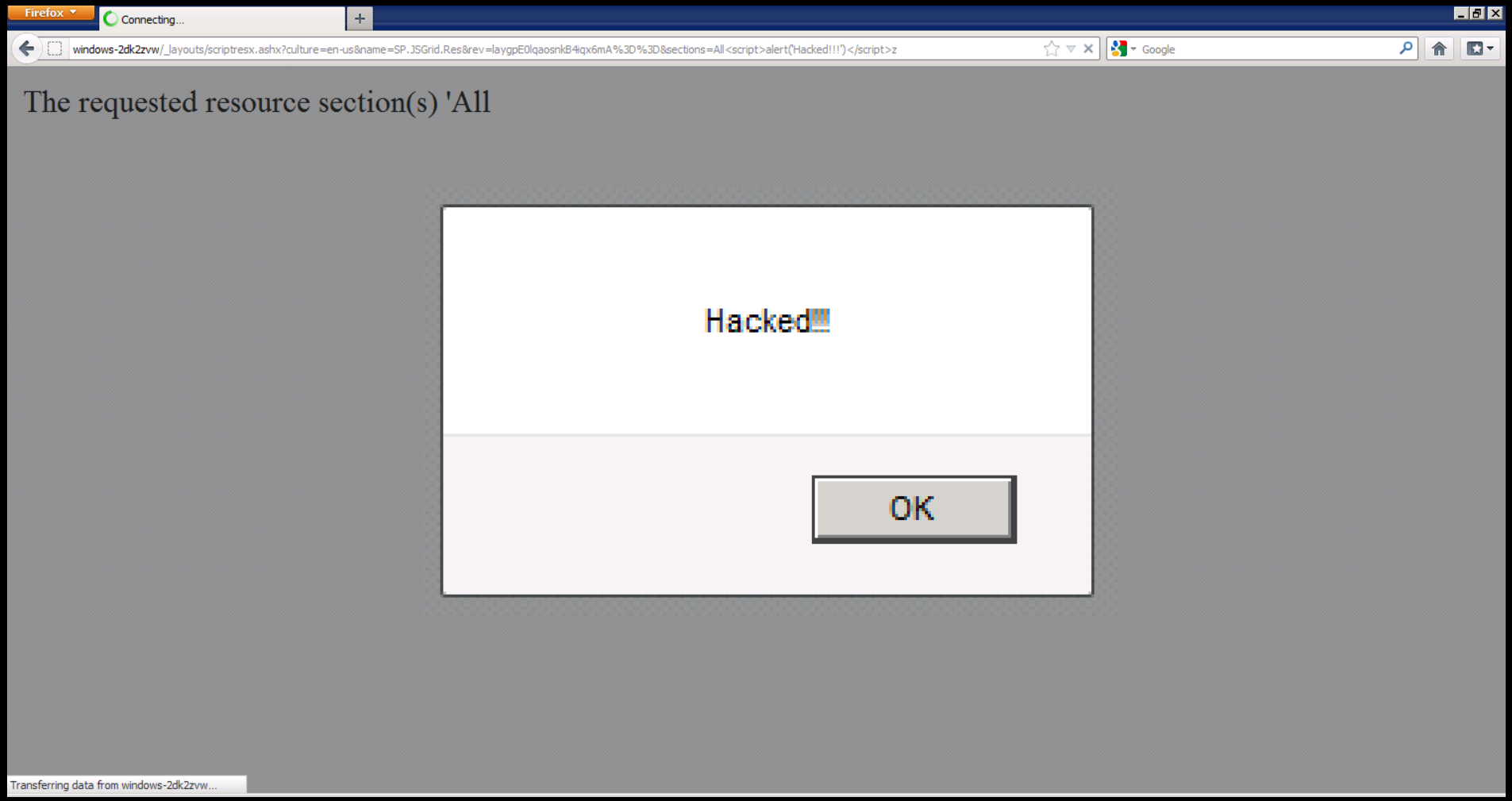




CVE-2012-1859

- A classic case of cross-site scripting vulnerability

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



OH SHIT

THERES NO ESCAPE

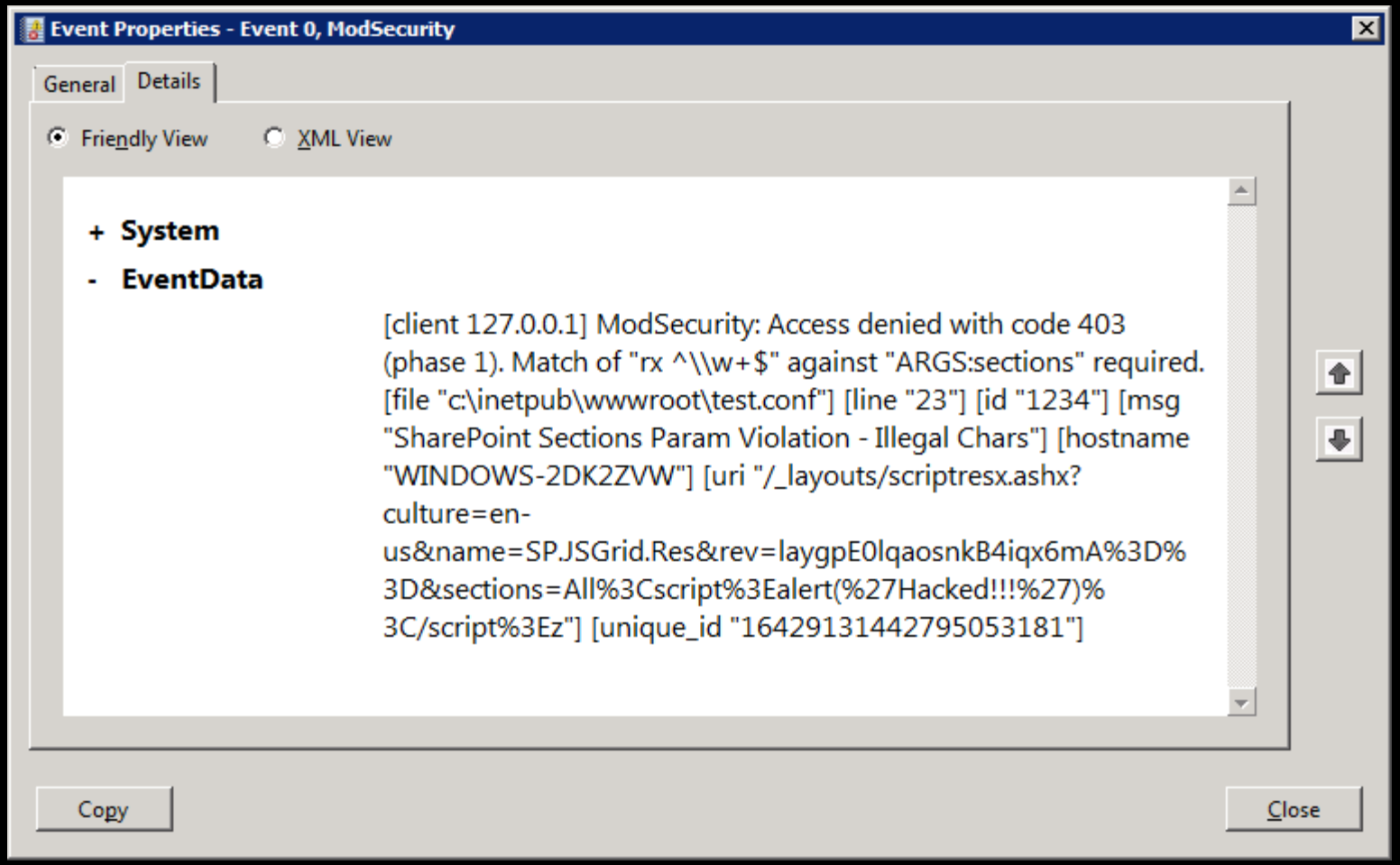
CVE-2012-1859

- 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/mod-security/files/modsecurity-apache/2.7.0-rc2/
- http://sourceforge.net/projects/mod-security/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

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

THANK YOU

FEEDBACK:

RBARNETT@MODSECURITY.ORG