ModSecurity: Embeddable Web Application Firewall

Ivan Ristic
ivanr@webkreator.com
+44 7766 508 210

Web Application Firewalls because...

- Most applications deployed today are insecure because the average developer is still not trained well enough.
- Web applications are inherently insecure because of the way they came to be.

- So, basically, we need any help we can get…

Introducing ModSecurity

- An open source web application firewall I started as a hobby back in late 2002: **http://www.modsecurity.org**
- Quite popular, with usage rising steadily.
- Commercially licensed and supported through **Thinking Stone**.

Positioning ModSecurity

- There's a limit to where being open source can take us - we need a good selling point.
- It's embeddable. This may be interesting!
  - Most WAFs are appliance-based and work in network mode.
  - That's fine (ModSecurity can work in network mode too).
  - But I like my WAF to be embeddable because...

Embeddable Web Application Firewalls

- No need to change your network.
- Easy to add, even easier to remove.
- Very low overhead.
- As scalable as the systems they work in.
- Do not introduce a point of failure.

ModSecurity: Major Features

- Real-time traffic monitoring.
  - It's an **IDS that understands HTTP really well** and has no problems with SSL-encrypted content.
- Logging.
  - Log the entire traffic stream. Or choose exactly what you want logged. **Useful to determine if a vulnerability has been exploited in the past.**
- Just-in-time patching.
  - Patch web application vulnerabilities externally to **reduce the window of opportunity**.

(**Mandatory disclaimer:** problems should be properly fixed whenever possible.)

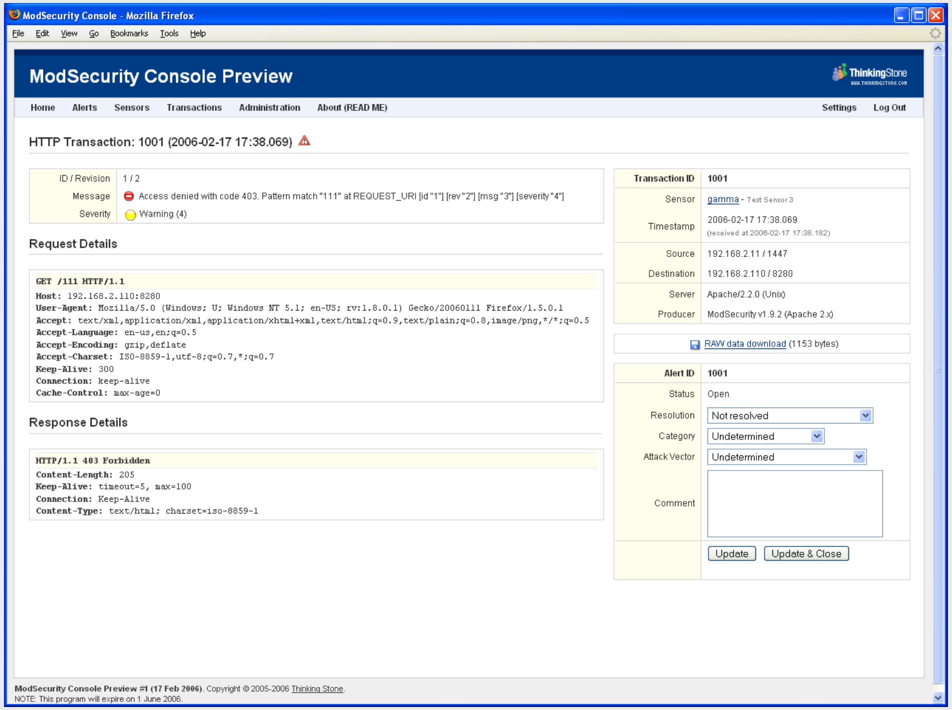
Product Range (1/2)

- Web server support:
  - Apache (1.3.x & 2.x) **- available now.**
  - Java-based web servers - **late Spring.**
  - Microsoft Internet Information Server (IIS) / Internet Security and Acceleration Server (ISA) - **late Summer.**

- **Standalone option** (when compiled with Apache 2.2.x and configured to work as reverse proxy).

Product Range (2/2)

- **ModSecurity Console** - **currently in private beta.**
  - Nice GUI.
  - Support for real-time logging and alert management.
  - Central management of all sensors.
  - Advanced features for security analysts.



ModSecurity Console Preview

HTTP Transaction: 1001 (2006-02-17 17:38.069) ⚠

ID / Revision	1 / 2
Message	⛔ Access denied with code 403. Pattern match "111" at REQUEST_URI [id "1"] [rev "2"] [msg "3"] [severity "4"]
Severity	● Warning (4)

Request Details

```
GET /111 HTTP/1.1
Host: 192.168.2.110:8280
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cache-Control: max-age=0
```

Response Details

```
HTTP/1.1 403 Forbidden
Content-Length: 205
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Transaction ID	1001
Sensor	gamma - Test Sensor 3
Timestamp	2006-02-17 17:38.069 (received at 2006-02-17 17:38.182)
Source	192.168.2.11 / 1447
Destination	192.168.2.110 / 8280
Server	Apache/2.2.0 (Unix)
Producer	ModSecurity v1.9.2 (Apache 2.x)

RAW data download (1153 bytes)

Alert ID	1001
Status	Open
Resolution	Not resolved
Category	Undetermined
Attack Vector	Undetermined
Comment	

ModSecurity Console Preview #1 (17 Feb 2006). Copyright © 2005-2006 Thinking Stone.
NOTE: This program will expire on 1 June 2006.

Questions?

Thank you!

Download this presentation from
http://www.thinkingstone.com/talks/

Ivan Ristic
ivanr@webkreator.com
+44 7766 508 210