

Securing and Managing the Oracle HTTP Server (706)

Real World Examples and Lessons Learned
Monday, May 4, 2009 01:15 - 02:15

Kevin Sheehan

Brian J. Mulreany

Agenda

- Today's Agenda:
 - Presenter Introductions
 - IOUG Membership Benefits
 - Defense in Depth & Role of Web Server
 - Scoring the OHS configuration
 - Hardening the OHS setup
 - Securing with mod_security and mod_rewrite
 - Questions and Answers

Presenter – Kevin Sheehan

- 28 years of IT experience
- 15 years Oracle experience with Oracle
- Currently Technical Director at Unisys
- Large Homeland Security Implementations
- Formerly Technical Director at Oracle
- Email: kpsheehan@gmail.com

Presenter – Brian Mulreany

- 20+ years of experience with Oracle Products
- 10+ years of experience with Web and Java technology
- Technical director with AT&T and Oracle Consulting focusing on software architecture
- Senior Architect with Unisys supporting DHS
- Email: bjm-uva@alumni.virginia.edu

IOUG Membership Benefits

- **Information**
 - Library of Oracle Knowledge
 - *SELECT Journal*
- **Education**
 - Collaborate Conferences
- **Networking**
 - Member Directory
 - Special Interest Groups
 - Discussion Forums
- **Advocacy**

Overview of Defense in Depth

- Layered approach to security
- No single point of security failure
- Secure ALL layers of the tech stack
- Applies to more than the technology
 - Hiring Practices (Background Investigations)
 - Procurement Practices
 - Security Awareness Training
- Ultimate goal is prevention but ...
- Secondary goal is to slow the attacker down

Is Your Web Server Vulnerable to Attack?

Because it sure is a target!

- **Gateway to your system**
- **Default configuration designed to serve and NOT protect**
- **Everything is servable content unless you take steps to block it**
- **Block everything and then open up only what is needed**



So just which OHS SHOULD You Install?



Picture Courtesy of cogdogblog's photostream on Flickr at <http://www.flickr.com/photos/cogdog/1576658693/>

©2009 Kevin Sheehan and Brian Mulreany. All Rights Reserved.

STOP! Don't pick *that* OHS

There are 10+ versions of OHS

"It is externally labeled as "10.1.3.3", but the component version is actually "10.1.3.1", and is a special build, different than the Oracle Application Server counterpart."

All OHS versions are not created equal

"Something to think about..."

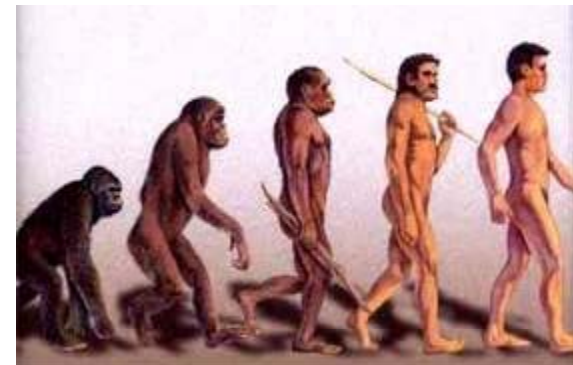
The Oracle HTTP Server delivered with the Oracle Database 10.2 Companion CD is provided for demonstration purposes, primarily for HTMLDB. However, its an older version with limited functionality and support. It also installs a mix of 10.2 and 10.1 products which is more difficult to maintain. Consider installing a better package of the Oracle HTTP Server."

OHS Version Guidelines

- Use App Server OHS, not DB version
- Use Stand-alone if possible
- Use Apache 2.0 if possible (if using Stand-alone)
- Use threaded MPM Worker if using Apache 2.0

How Our Web Tier Evolved with apologies to Darwin (& chimpanzees)

- 6 years ago - Chimps (Chumps?)
 - J2EE/Portal Install
 - Shutdown everything but Webcache
 - Unneeded software
- 3 years ago – Neanderthals
 - Standalone Webcache
 - Single Threaded – Not scalable
 - No reverse proxy or application firewall
- 2 years ago – Homo Sapiens
 - Standalone OHS – Apache 2.0



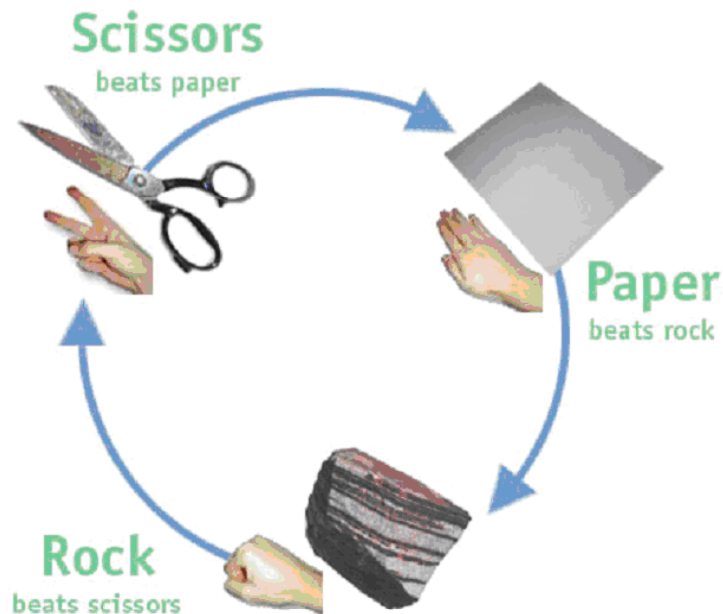
Introducing CIS

- Center for Internet Security (CIS) benchmark
- Checking configuration vs. actual scanning
- Guess the CIS score after default install
- Improving your security and your CIS score
 - How many IDs does it take to run OHS?
 - HTTP Headers and Error Documents
 - Basic OHS hardening
 - Lock down those load modules
 - Hardening with `mod_security` or `mod_rewrite`

OHS Baseline CIS Score

```
#===== [ CIS Apache Benchmark Scoring Tool 2.10 ] =====#  
[Section 1.14] Web Server Software Obfuscation General Directives  
[FAILED] ServerSignature is "On"  
[Section 1.18] Access Control Directives  
[PASSED] Directory entry for "/" is properly configured. allowoverride None  
[FAILED] Directory entry for "/" is not properly configured. options FollowSymLinks  
[FAILED] Directive "deny" Directory entry for "/" is not defined.  
[Section 1.20] Directory Functionality/Features Directives  
[FAILED] Did not disable Option directive "Includes" for DocumentRoot  
[Section 1.21] Limiting HTTP Request Methods  
[FAILED] There is no LimitExcept directive for DocumentRoot  
[Section 1.23] Remove Default/Unneeded Apache Files  
[VERIFY] Verify DocumentRoot files are not default Apache files.  
...  
[Apache Benchmark Score]: 2.79 out of 10.00]
```

Fingerprinting



- What if you knew what weapon to use?
- Fingerprinting tries to identify the configuration
- Attacks use known vulnerabilities
- Stop information leaks

Fingerprinting OHS Base Install

host	port	ssl	banner reported	banner deduced	icon	confidence
192.168.0.12	7777		Oracle-Application-Server-10g/10.1.3.1.0 Oracle-HTTP-Server	Apache/2.0.x		

SSL analysis

httpprint © 2003-2005 net-square

Fingerprinting tool has identified the default install as Apache 2.0 with a high degree of confidence.

How many User IDs does it take to run OHS?

“Two-Man Rule” or “Four-Eyes Principle”

A security control technique that requires more than one person or more than one user ID to compromise an entire system.

It takes **three** User IDs to run OHS.

1. One user ID to own the OHS software
2. One user ID to run the OHS web software
3. One user ID to own the web content

Modify Headers and Error Pages

Basic Header

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Mon, 23 Feb 2009 02:19:58 GMT

Server: Oracle-Application-Server-
10g/10.1.3.1.0 Oracle-HTTP-Server

Error Page

<body>

<h1>Not Found</h1>

<p>The requested URL /notfound was not
found on this server.</p>

<hr>

<address>Oracle-Application-Server-
10g/10.1.3.1.0 Oracle-HTTP-Server
Server at bjm-desktop Port 80</address>

</body>

- HTTP headers after default install identifies web server
- Default error pages show web server version, hostname, and port
- May show internal information if using a reverse proxy

HTTP headers – Leave no trace

Original Configuration

ServerAdmin you@example.com
ServerName bjm-desktop
ServerTokens Minimal
Limit on OPTIONS method

No fake headers to obfuscate server
and modify order of headers

Using default error pages

Revised Configuration

```
###ServerAdmin you@example.com  
ServerName ohs.collaborate09.org  
ServerTokens None  
<LimitExcept GET POST>  
    deny from all  
</LimitExcept>  
Options None  
Header onsuccess set X-Powered-By "ASP.NET"  
  
ErrorDocument 403 /error_contactus.htm  
ErrorDocument 500 "There was an error  
processing your request, please retry."
```

HTTP headers – after revisions

HTTP/1.1 403 Forbidden

Date: Sun, 01 Mar 2009 16:07:11 GMT

X-Cache: MISS from proxy.domain.com

Last-Modified: Sun, 01 Mar 2009 15:56:50 GMT

ETag: "307d5-a0-bffb1480"

Content-Length: 160

X-Powered-By: ASP.NET

X-AspNet-Version: 1.1.4322

Content-Type: text/html

```
<HTML><HEAD><TITLE>Error – Contact Us</TITLE>
```

```
</HEAD><BODY>
```

```
<H1>There was an error processing your  
request</H1>
```


```
</BODY></HTML>
```

- Headers and error page content has been scrubbed
- Don't forget to remove demo content too.

Fingerprinting Revised Setup

host	port	ssl	banner reported	banner deduced	icon	confidence
192.168.0.12	7777		-	Orion/2.0x		<div style="width: 10%; height: 10px; background-color: blue;"></div>

SSL analysis

 httpprint © 2003-2005 net-square

After revising headers and error pages the fingerprinting tool guesses that the web server is Orion and reports a low degree of confidence.

Lock down those load modules

- Determine how OHS is being used:
Application server front-end, Apex front-end,
Reverse Proxy, 11i Application Front-end ...
- Evaluate which load modules are required
based on intended use
- Disable those modules that are not required

Disable Unused Load Modules

Original Configuration	Revised Configuration
LoadModule status_module	LoadModule status_module
LoadModule autoindex_module	###LoadModule autoindex_module
LoadModule dir_module	###LoadModule dir_module
LoadModule imap_module	###LoadModule imap_module
LoadModule alias_module	LoadModule alias_module
LoadModule php4_module	###LoadModule php4_module
LoadModule expires_module	LoadModule expires_module
LoadModule rewrite_module	LoadModule rewrite_module
N/A	LoadModule security_module

*CIS flagged modules shown in red

Mod_Security vs Mod_Rewrite

Mod_security

- Pro
 - Availability of Rules
 - Detailed logging
 - Designed as a security tool
- Con
 - New module to maintain
 - Parsing adds overhead
 - OHS uses old 1.84 version

Mod_rewrite

- Pro
 - Typically already in use
 - Good for simple blocking
 - Performance
- Con
 - More work to code rules
 - Logging more for debug
 - Not designed for security

Compare Blocking Put Method

Mod_rewrite Rule

```
RewriteCond  
%{REQUEST_METHOD}  
^PUT  
RewriteRule .* - [F]
```

Mod_security Rule

```
SecFilterSelective  
REQUEST_METHOD  
"PUT"  
"id:888000,deny,log,  
status:405,msg:  
'PUT method denied'"
```

Default Logging - Minimal

Default Common Logging format:

LogFormat "%h %l %u %t \"%r\" %>s %B

Default Common Logging result:

192.168.0.10 - - [23/Feb/2009:21:45:58 -0500] "GET /index.html
HTTP/1.1" 200 14679

Blackbox + access log format

Blackbox + access log format:

```
LogFormat "%h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\" \"%{X-FORWARDED-FOR}i\" \"%{cookie}i\" %v %X  
%P %T" blackbox
```

Blackbox + access log result:

```
192.168.0.10 - - [10/Mar/2009:21:23:17 -0400] "GET /index.html  
HTTP/1.1" 200 14679  
"http://192.168.0.12:7777/OHSDemos.htm" "Mozilla/4.0  
(compatible; MSIE 7.0; Windows NT 6.0; GTB5; SLCC1; .NET  
CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.5.30729;  
.NET CLR 3.0.30618)" "10.0.0.100"  
"JSESSIONID=8EEEE08C4DEFF1B72F9BCCEC72B58544"  
bjm-desktop + 27860 0
```

Case Study – The attack

- Big increase in 403 not authorized requests
- Big increase in 404 not found requests
- Big increase in 400 Bad Request or 406 Not Acceptable requests
- Unusual 404 pattern, not favicon.ico
- Hundreds of requests per minute off-peak
- Many requests from one IP in under a minute
- Requests for unused technology, PHP
- Non-standard user-agent

Case Study – The analysis

- OHS access log showed the requests coming from user-agent w3af.sourceforge.net
- Web search found:
 - w3af is a Web Application Attack and Audit framework. The project's goal is to create a framework to find and exploit web application vulnerabilities that is easy to use and extend.

Case Study – The response

- Added new mod_security rule
- SecFilterSelective HTTP_USER_AGENT
"w3af\.sourceforge\.net"
"id:888000,deny,log,status:406,msg:'User Agent invalid'"
- The rule blocks access by the user agent w3af and returns a 406 Not Acceptable response. Blocked request information is logged in the mod_security log.
- Added rule to list of user agent blocking rules

Final CIS Score

[Apache Benchmark Score]: 8.14 out of 10.00]

[Section 1.9] Configure the Apache Software

[FAILED] Unless required, module "mod_status" should not be compiled into Apache.

[Section 1.11] Server Oriented General Directives

[FAILED] HostnameLookups is off for Apache Web Server

[Section 1.13] Denial of Service (DoS) Protective General Directives

[FAILED] Timeout value "300" is greater than the recommended "60"

[Section 1.24] Update Ownership and Permissions for Enhanced Security

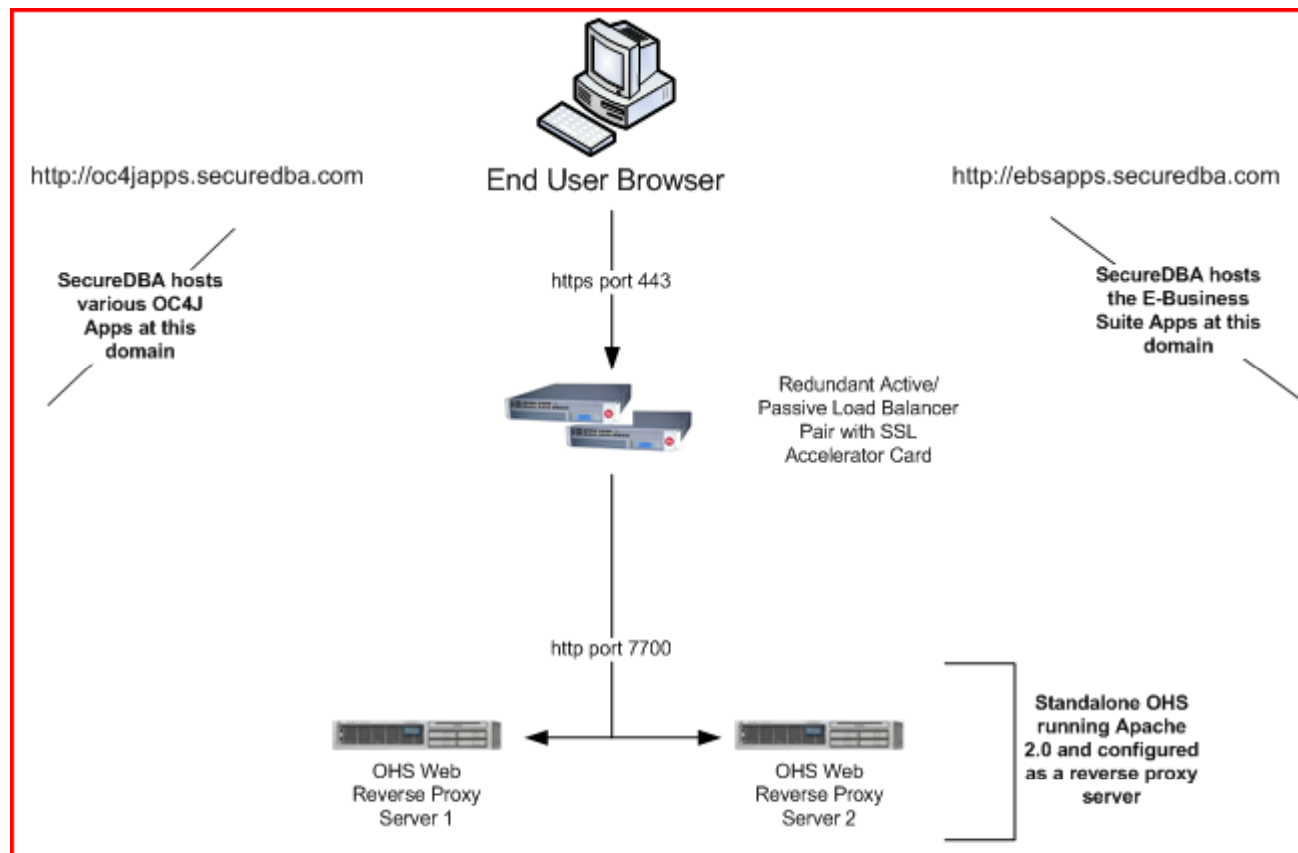
[FAILED] Owner of Log directory should be root.

Configure an OHS reverse proxy

A reverse proxy server is an instance of OHS that:

- takes an inbound HTTP request and forwards it to your web servers thus providing a layer of obfuscation
- based on rules you define, either passes (proxies) a request onward or denies it access and therefore you can configure if to limit probes by individuals trying to fingerprint your environment
- can serve up static content to take some load off of your web/application servers
- can act as a server-side cache
- can compress content

Configure an OHS reverse proxy



Tips & Tricks for Managing OHS

Best Feature of OHS 2 not enabled

Build your own moat

Listen up!

Use an inclusive OHS configuration

Can you use mod_plsql and OHS2

Use mod_rewrite or mod_security?

A bit of nostalgia

Virtualization

Load Module order is important

Test those changes

Need a little Cache?

Terminating SSL in front of OHS

→Use threads with mpm worker

→Protect your COTS products

→Make sure you check all ports

→Use include to separate configs

→Yes, and reduce DB connections

→Why choose, use both

→New load modules with 2.2

→Inherit rules with Virtualhosts

→Load Module order matters in 1.3

→apachectl configtest is OK

→Take advantage of client caching

→Speed up your secure requests

Thanks for Attending!

Contact Information

Kevin Sheehan

Email: kpsheehan@gmail.com

Brian J. Mulreany

Email: bjm-uva@alumni.virginia.edu

Web Site: <http://securedba.com>

Remember to fill out a survey please!