OWASP
Open Web Application
Security Project

Your web server has been hacked now what?

Archzilon Eshun-Davies (@laudarch)

CISO/CEO Tactical Intelligence Security

OWASP Ghana 2019

OWASP
Open Web Application
Security Project

Who is this talk for?

- Individuals, developers and sys admins.

Are you sure you’ve been hacked?

Q1: Does your site look suspiciously different?

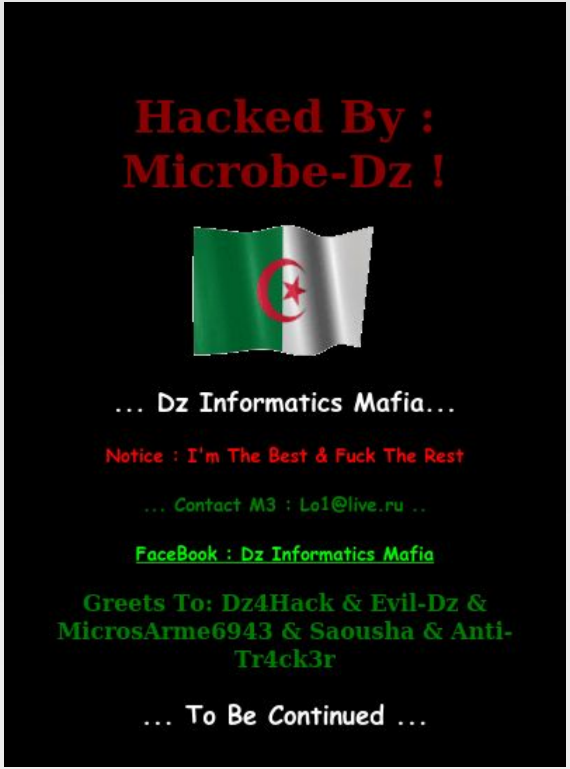
Q2: Did your bandwidth usage shoot up?

Q3: Are your customers complaining of strange calls?

Q4: Have you lost money?

Yes you have

You can tell because well it looks like this or similar.



Hacked By :
Microbe-Dz !

... Dz Informatics Mafia...

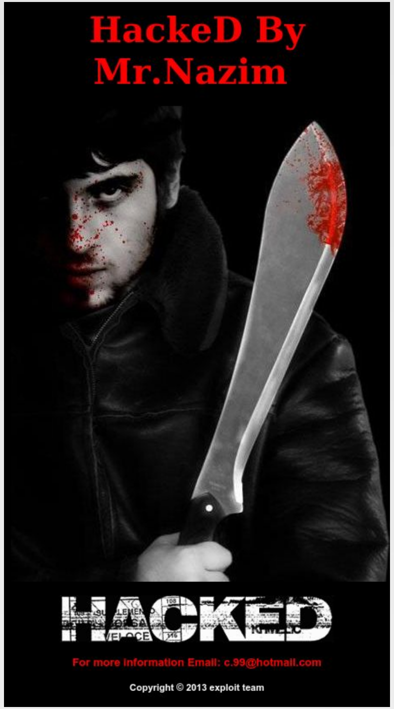
Notice : I'm The Best & Fuck The Rest

... Contact M3 : Lo1@live.ru ..

FaceBook : Dz Informatics Mafia

Greets To: Dz4Hack & Evil-Dz & MicrosArme6943 & Saousha & Anti-Tr4ck3r

... To Be Continued ...



HackeD By
Mr.Nazim

For more information Email: c.99@hotmail.com

Copyright © 2013 exploit team

How did they get in?

Logs: Log files in /var/log, error_log.

Check you app: PHP, JS, CSS, PDFs, files - If you have baseline here it'll help a **lot**.

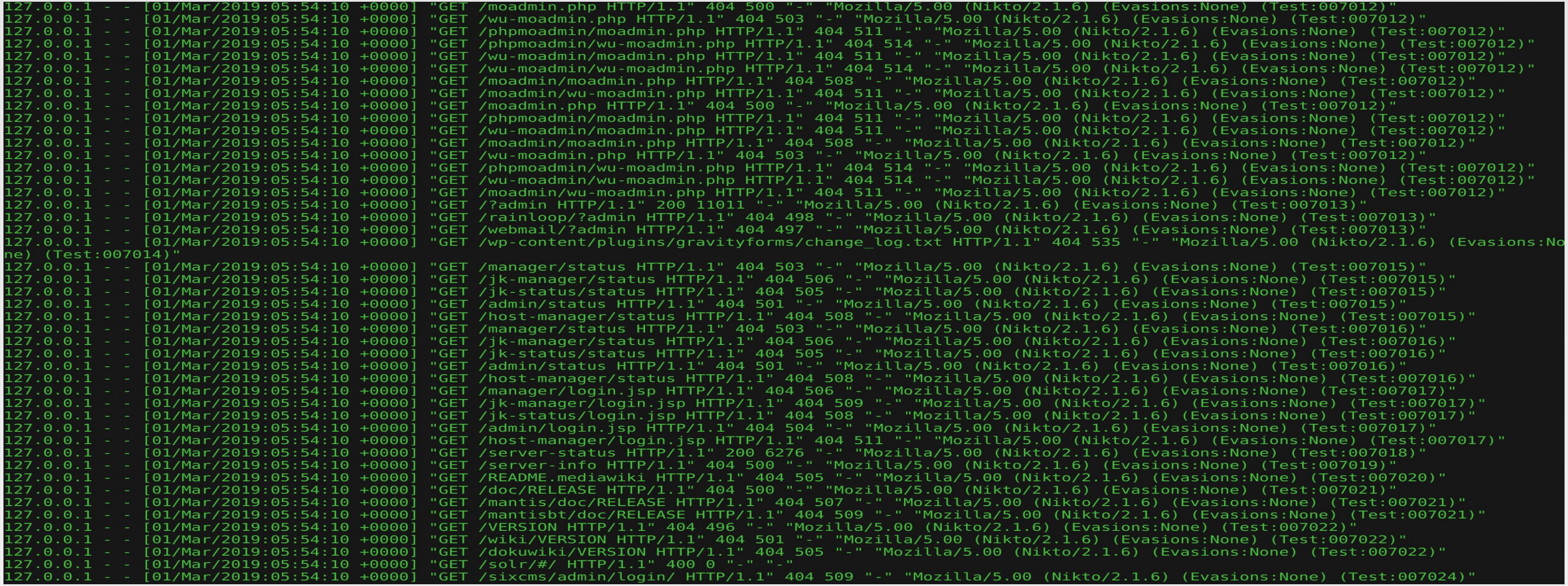
Forensics: File dates, permissions, sizes, access date and time etc

Database: Check your database for funny queries and injected queries and procedures.

Check developers workstations.

Cron Jobs: Check cron jobs for unusual jobs. Someone compromising a system will often leave a backdoor to get back in again and again. Cron is a very popular way to do this if they managed to get that far.

How does it look like?

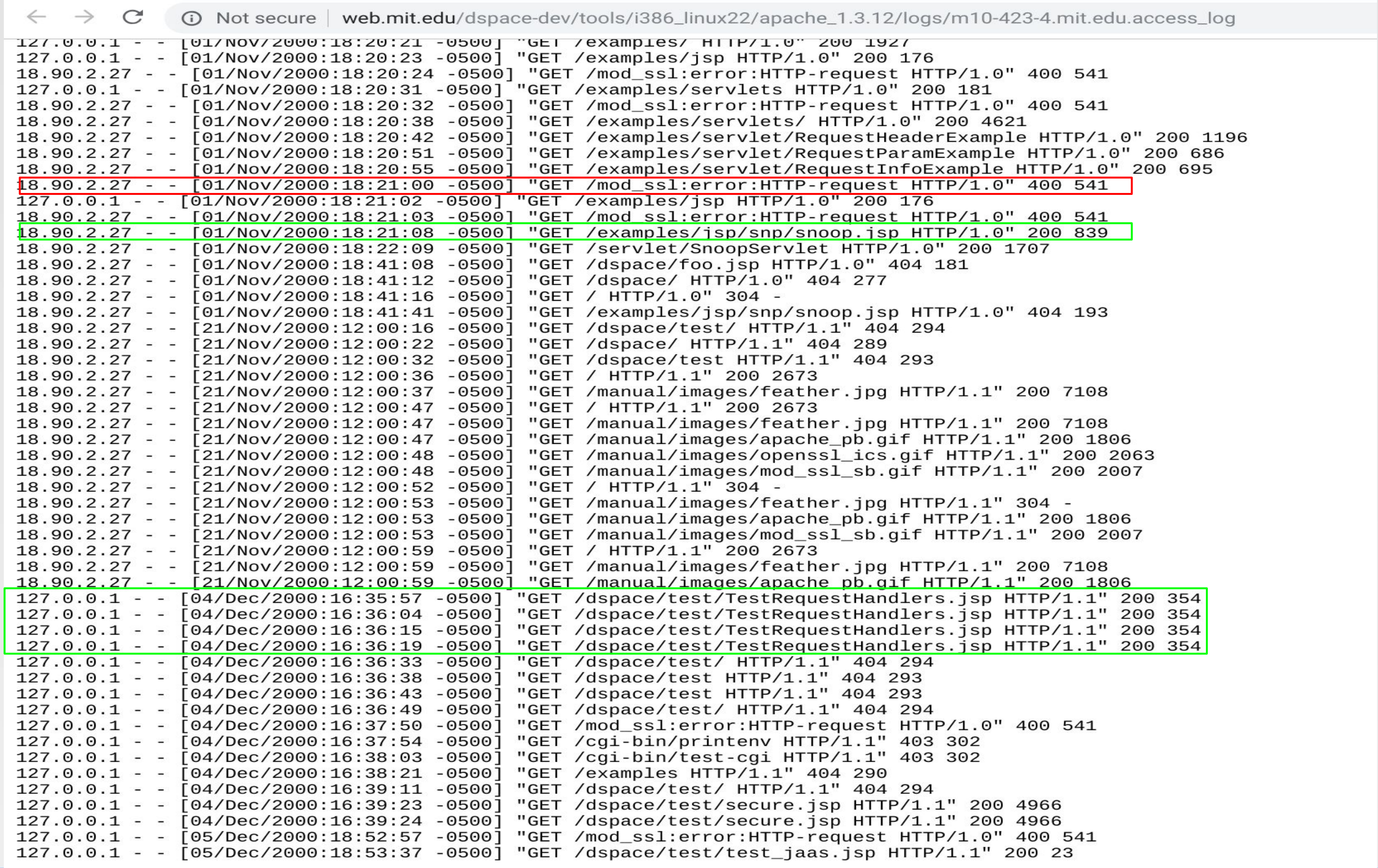


```
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /moadmin.php HTTP/1.1" 404 500 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wu-moadmin.php HTTP/1.1" 404 503 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /phpmoadmin/moadmin.php HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /phpmoadmin/wu-moadmin.php HTTP/1.1" 404 514 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wu-moadmin/moadmin.php HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wu-moadmin/wu-moadmin.php HTTP/1.1" 404 514 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /moadmin/moadmin.php HTTP/1.1" 404 508 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /moadmin/wu-moadmin.php HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /moadmin.php HTTP/1.1" 404 500 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /phpmoadmin/moadmin.php HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wu-moadmin/moadmin.php HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /moadmin/moadmin.php HTTP/1.1" 404 508 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wu-moadmin.php HTTP/1.1" 404 503 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /phpmoadmin/wu-moadmin.php HTTP/1.1" 404 514 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wu-moadmin/wu-moadmin.php HTTP/1.1" 404 514 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /moadmin/wu-moadmin.php HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007012)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /?admin HTTP/1.1" 200 11011 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007013)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /rainloop/?admin HTTP/1.1" 404 498 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007013)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /webmail/?admin HTTP/1.1" 404 497 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007013)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wp-content/plugins/gravityforms/change_log.txt HTTP/1.1" 404 535 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:No
ne) (Test:007014)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /manager/status HTTP/1.1" 404 503 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007015)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /jk-manager/status HTTP/1.1" 404 506 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007015)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /jk-status/status HTTP/1.1" 404 505 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007015)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /admin/status HTTP/1.1" 404 501 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007015)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /host-manager/status HTTP/1.1" 404 508 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007015)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /manager/status HTTP/1.1" 404 503 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007016)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /jk-manager/status HTTP/1.1" 404 506 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007016)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /jk-status/status HTTP/1.1" 404 505 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007016)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /admin/status HTTP/1.1" 404 501 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007016)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /host-manager/status HTTP/1.1" 404 508 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007016)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /manager/login.jsp HTTP/1.1" 404 506 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007017)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /jk-manager/login.jsp HTTP/1.1" 404 509 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007017)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /jk-status/login.jsp HTTP/1.1" 404 508 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007017)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /admin/login.jsp HTTP/1.1" 404 504 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007017)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /host-manager/login.jsp HTTP/1.1" 404 511 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007017)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /server-status HTTP/1.1" 200 6276 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007018)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /server-info HTTP/1.1" 404 500 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007019)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /README.mediawiki HTTP/1.1" 404 505 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007020)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /doc/RELEASE HTTP/1.1" 404 500 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007021)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /mantis/doc/RELEASE HTTP/1.1" 404 507 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007021)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /mantisbt/doc/RELEASE HTTP/1.1" 404 509 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007021)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /VERSION HTTP/1.1" 404 496 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007022)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /wiki/VERSION HTTP/1.1" 404 501 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007022)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /dokuwiki/VERSION HTTP/1.1" 404 505 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007022)"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /solr/#/ HTTP/1.1" 400 0 "-" "-"
127.0.0.1 - - [01/Mar/2019:05:54:10 +0000] "GET /sixcms/admin/login/ HTTP/1.1" 404 509 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007024)"
```

404 Good, 200 Bad

We can follow attack patterns to see when they succeeded and where.

While you go through logs you are looking for how and where they succeeded.



Not secure | web.mit.edu/dspace-dev/tools/i386_linux22/apache_1.3.12/logs/m10-423-4.mit.edu.access_log

```
127.0.0.1 - - [01/Nov/2000:18:20:21 -0500] "GET /examples/ HTTP/1.0" 200 1927
127.0.0.1 - - [01/Nov/2000:18:20:23 -0500] "GET /examples/jsp HTTP/1.0" 200 176
18.90.2.27 - - [01/Nov/2000:18:20:24 -0500] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 541
127.0.0.1 - - [01/Nov/2000:18:20:31 -0500] "GET /examples/servlets HTTP/1.0" 200 181
18.90.2.27 - - [01/Nov/2000:18:20:32 -0500] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 541
18.90.2.27 - - [01/Nov/2000:18:20:38 -0500] "GET /examples/servlets/ HTTP/1.0" 200 4621
18.90.2.27 - - [01/Nov/2000:18:20:42 -0500] "GET /examples/servlet/RequestHeaderExample HTTP/1.0" 200 1196
18.90.2.27 - - [01/Nov/2000:18:20:51 -0500] "GET /examples/servlet/RequestParamExample HTTP/1.0" 200 686
18.90.2.27 - - [01/Nov/2000:18:20:55 -0500] "GET /examples/servlet/RequestInfoExample HTTP/1.0" 200 695
18.90.2.27 - - [01/Nov/2000:18:21:00 -0500] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 541
127.0.0.1 - - [01/Nov/2000:18:21:02 -0500] "GET /examples/jsp HTTP/1.0" 200 176
18.90.2.27 - - [01/Nov/2000:18:21:03 -0500] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 541
18.90.2.27 - - [01/Nov/2000:18:21:08 -0500] "GET /examples/jsp/snp/snoop.jsp HTTP/1.0" 200 839
18.90.2.27 - - [01/Nov/2000:18:22:09 -0500] "GET /servlet/SnoopServlet HTTP/1.0" 200 1707
18.90.2.27 - - [01/Nov/2000:18:41:08 -0500] "GET /dspace/foo.jsp HTTP/1.0" 404 181
18.90.2.27 - - [01/Nov/2000:18:41:12 -0500] "GET /dspace/ HTTP/1.0" 404 277
18.90.2.27 - - [01/Nov/2000:18:41:16 -0500] "GET / HTTP/1.0" 304 -
18.90.2.27 - - [01/Nov/2000:18:41:41 -0500] "GET /examples/jsp/snp/snoop.jsp HTTP/1.0" 404 193
18.90.2.27 - - [21/Nov/2000:12:00:16 -0500] "GET /dspace/test/ HTTP/1.1" 404 294
18.90.2.27 - - [21/Nov/2000:12:00:22 -0500] "GET /dspace/ HTTP/1.1" 404 289
18.90.2.27 - - [21/Nov/2000:12:00:32 -0500] "GET /dspace/test HTTP/1.1" 404 293
18.90.2.27 - - [21/Nov/2000:12:00:36 -0500] "GET / HTTP/1.1" 200 2673
18.90.2.27 - - [21/Nov/2000:12:00:37 -0500] "GET /manual/images/feather.jpg HTTP/1.1" 200 7108
18.90.2.27 - - [21/Nov/2000:12:00:47 -0500] "GET / HTTP/1.1" 200 2673
18.90.2.27 - - [21/Nov/2000:12:00:47 -0500] "GET /manual/images/feather.jpg HTTP/1.1" 200 7108
18.90.2.27 - - [21/Nov/2000:12:00:47 -0500] "GET /manual/images/apache_pb.gif HTTP/1.1" 200 1806
18.90.2.27 - - [21/Nov/2000:12:00:48 -0500] "GET /manual/images/openssl_ics.gif HTTP/1.1" 200 2063
18.90.2.27 - - [21/Nov/2000:12:00:48 -0500] "GET /manual/images/mod_ssl_sb.gif HTTP/1.1" 200 2007
18.90.2.27 - - [21/Nov/2000:12:00:52 -0500] "GET / HTTP/1.1" 304 -
18.90.2.27 - - [21/Nov/2000:12:00:53 -0500] "GET /manual/images/feather.jpg HTTP/1.1" 304 -
18.90.2.27 - - [21/Nov/2000:12:00:53 -0500] "GET /manual/images/apache_pb.gif HTTP/1.1" 200 1806
18.90.2.27 - - [21/Nov/2000:12:00:53 -0500] "GET /manual/images/mod_ssl_sb.gif HTTP/1.1" 200 2007
18.90.2.27 - - [21/Nov/2000:12:00:59 -0500] "GET / HTTP/1.1" 200 2673
18.90.2.27 - - [21/Nov/2000:12:00:59 -0500] "GET /manual/images/feather.jpg HTTP/1.1" 200 7108
18.90.2.27 - - [21/Nov/2000:12:00:59 -0500] "GET /manual/images/apache_pb.gif HTTP/1.1" 200 1806
127.0.0.1 - - [04/Dec/2000:16:35:57 -0500] "GET /dspace/test/TestRequestHandlers.jsp HTTP/1.1" 200 354
127.0.0.1 - - [04/Dec/2000:16:36:04 -0500] "GET /dspace/test/TestRequestHandlers.jsp HTTP/1.1" 200 354
127.0.0.1 - - [04/Dec/2000:16:36:15 -0500] "GET /dspace/test/TestRequestHandlers.jsp HTTP/1.1" 200 354
127.0.0.1 - - [04/Dec/2000:16:36:19 -0500] "GET /dspace/test/TestRequestHandlers.jsp HTTP/1.1" 200 354
127.0.0.1 - - [04/Dec/2000:16:36:33 -0500] "GET /dspace/test/ HTTP/1.1" 404 294
127.0.0.1 - - [04/Dec/2000:16:36:38 -0500] "GET /dspace/test HTTP/1.1" 404 293
127.0.0.1 - - [04/Dec/2000:16:36:43 -0500] "GET /dspace/test HTTP/1.1" 404 293
127.0.0.1 - - [04/Dec/2000:16:36:49 -0500] "GET /dspace/test/ HTTP/1.1" 404 294
127.0.0.1 - - [04/Dec/2000:16:37:50 -0500] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 541
127.0.0.1 - - [04/Dec/2000:16:37:54 -0500] "GET /cgi-bin/printenv HTTP/1.1" 403 302
127.0.0.1 - - [04/Dec/2000:16:38:03 -0500] "GET /cgi-bin/test-cgi HTTP/1.1" 403 302
127.0.0.1 - - [04/Dec/2000:16:38:21 -0500] "GET /examples HTTP/1.1" 404 290
127.0.0.1 - - [04/Dec/2000:16:39:11 -0500] "GET /dspace/test/ HTTP/1.1" 404 294
127.0.0.1 - - [04/Dec/2000:16:39:23 -0500] "GET /dspace/test/secure.jsp HTTP/1.1" 200 4966
127.0.0.1 - - [04/Dec/2000:16:39:24 -0500] "GET /dspace/test/secure.jsp HTTP/1.1" 200 4966
127.0.0.1 - - [05/Dec/2000:18:52:57 -0500] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 541
127.0.0.1 - - [05/Dec/2000:18:53:37 -0500] "GET /dspace/test/test_jaas.jsp HTTP/1.1" 200 23
```

All IPs are liars.

Implement your own logger take all IPs

```
$ip[] = $_SERVER['HTTP_CLIENT_IP'];

$ip[] = $_SERVER['HTTP_X_FORWARDED_FOR'];

$ip[] = $_SERVER['REMOTE_ADDR'];
```

You might just get the real IP from the proxy.

How to prevent the hack

- Harden servers, including using vendor recommendations on secure configurations
- Code review and testing.
- Have your web app / web site vulnerability tested by a professional certified tester at least once.
- Use Intrusion Prevention Systems.
- Check out OWASP www.owasp.org and http://phpsec.org/projects/guide/2.html for web application security resources.

KEEP
CALM
AND
ASK
QUESTIONS