

Re: Looking for help against Chinese Hacking Team

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-12/msg00217.html>

- *From:* p4ssion <p4ssion@xxxxxxxx>
 - *Date:* Fri, 19 Dec 2008 10:14:28 +0900
-

Also they are using cookie. it doesn't appear at Web log file.
Nowaday we can't find clue for attack.

Finding weak web source and Fix validation problem is best way.

On Fri, Dec 19, 2008 at 12:00 AM, David Howe
<DaveHowe.Pentest@xxxxxxxxxxxxxxxx> wrote:

Mike wrote:

On Dec 16, 2008, at 5:53 AM, Adriel T. Desautels wrote:

If he's looking to stop attacks then he needs to remove the vector through which he is being attacked. IPS devices do not remove the vector, they make an attempt to prevent the vector from being accessed. While I support the use of properly configured and maintained IPS technologies, I'd never recommend using them as a method for remediation because they are only a method for mitigation. Sure mitigation is great, but its not a fix.

A lot of good advice has been offered, but in order to spot what happened, somebody will have to examine the web server logs to look for evidence of SQL injection or whatever method was used to exploit the application.

With that in mind, here are some examples of SQL injection that might be useful (from Apache logs):

```
atta.cker.ip.address www.vulnerableserver.com - [13/Apr/
2008:04:23:43-0800] "GET /index.php?go=detail&id=-99999/**/union/**/
select/**/0,0,0,0,0,0,0,0,0,0x7c,email,0x3a,concat(username,
```

Re: Looking for help against Chinese Hacking Team

0x3a,password),1,1,1,1,1,2,2,2,2,2/**/from/*<http://www.hackedserver.com/html/images/idd.txt>?
??? HTTP/1.1" 200 63919 "-" "libwww-perl/5.811"

atta.cker.ip.address -- [13/Apr/2008:04:23:43 -0800] "GET /?
article=63+and+(select+ascii(substring(cast(+table%5fname+as+char,
+3,+1))%2616+from+information%5fschema.tables+where+table%5ftype+%3c%3e
+(concat(char(118),char(105),char(101),char(119))))+and+1=1++limit
+1)HTTP/1.0" 200 53604 "-" "Opera/9.23 (Windows NT 5.1; U; en)"

I find most injection attacks these days attempt to use cloaking techniques – hence you should look for patterns like using the cast function on a large hex block, then the exec function...

simpler yet, almost no valid log entries should have --- or ; in them; few should have single quotes, either.

This list is sponsored by: Cenzic

Security Trends Report from Cenzic
Stay Ahead of the Hacker Curve!
Get the latest Q2 2008 Trends Report now

www.cenzic.com/landing/trends-report

~~~~~  
p4ssionable Security explorer ! p4ssion  
E-mail: p4ssion@xxxxxxxxx ,  
~~~~~

This list is sponsored by: Cenzic

Security Trends Report from Cenzic
Stay Ahead of the Hacker Curve!
Get the latest Q2 2008 Trends Report now

www.cenzic.com/landing/trends-report
