#BugBounty — API keys leakage, Source code disclosure in India's largest e-commerce health care company.

Avinash Jain (@logicbomb_1) Follow
Feb 25, 2018 · 3 min read

Hi Guys,

Back with a long pending vulnerability that I found during my bug bounty hunt, though a late blog but I found it worth sharing. I have found this vulnerability in ***India's largest online health platform website.***

> *By this vulnerability, I was able to read source code of the application , sensitive files like webconfig where I got APIs key of mail server, sms, payment gateway etc and further I was also able to use these mail server key to send mail from their*

> *enterprise mail server and were even able to send sms using the sms keys to thier customers. Let's see how I was able to do so —*

The technique that was used to find this vulnerability was Path Traversal Attack.

Vulnerable URL

I found this vulnerability in the URL and the parameter as shown in the screenshot above.

The response of the above URL HTTP request was as below-

Vulnerable Request response

If you look at the screenshot above, you will see the HTTP header “Server” . By this I analysed that Microsoft-IIS web server is in use. So I tried to open WIN.INI file of windows by path traversal attack.

Path traversal atatck

And I got the following response-

HTTP Response

This is the content of WIN.INI file. So by this I was confirmed that Local File Inclusion vulnerability exist. So I tried escalating this vulnerability and went on to read some source code of the application —

Login page source code request

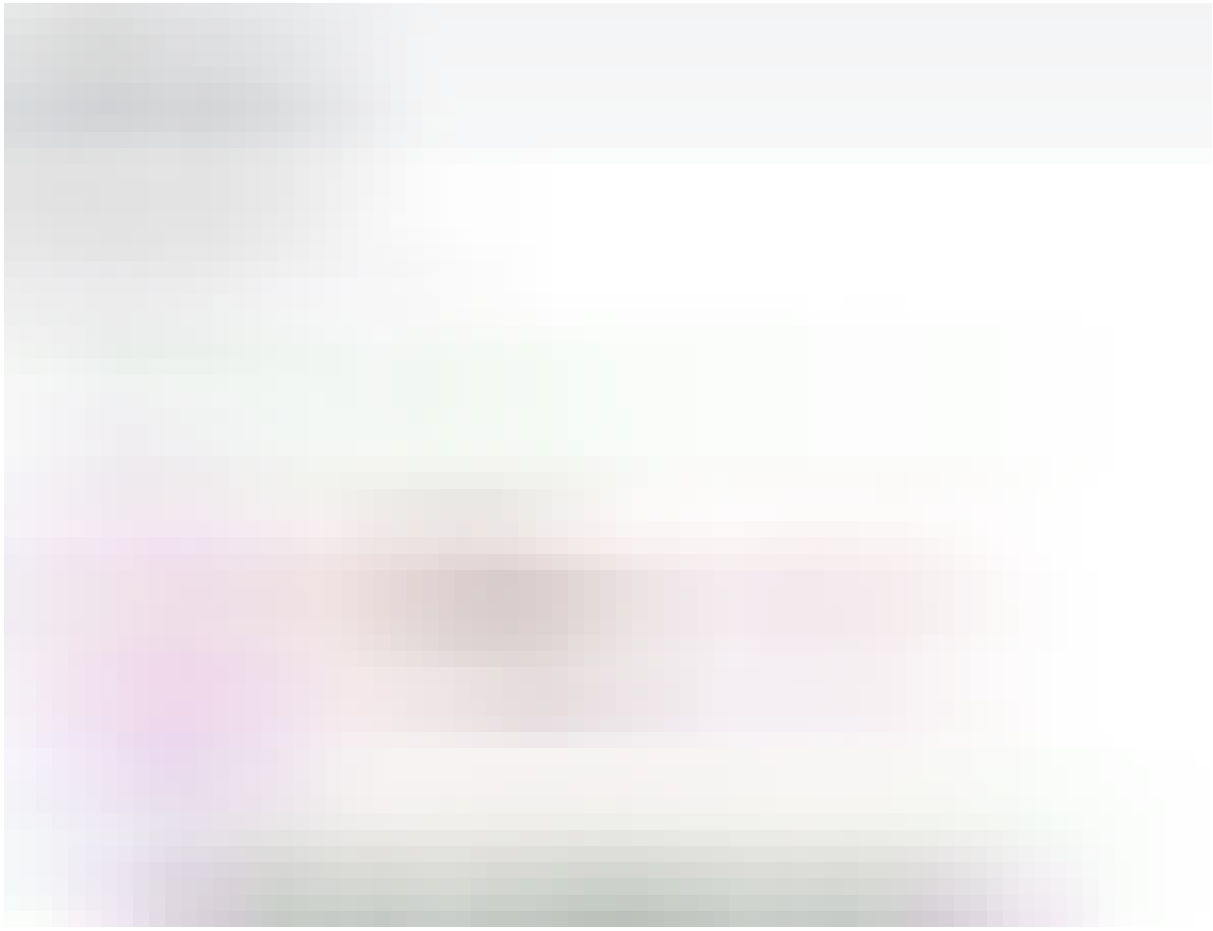
As I knew it was an IIS server so I was clear about how application directory looks like and I tried reading source code of login page and as expected I got the below response —

Login page source code

Similarly , I was able to download the complete source code of the application of any page. Now comes the critical aspect of this, the web.config file is below –

Web Config file inclusion

and when I saw the response of the above request, I had a huge smile on my face :D



All the sensitive APIs key were exposed!- Mail server API key, IIS server admin credentials , SMS API keys, Payment Gateway Keys and this was something really critical. I was able to use these keys to send mails, send SMS to user, payment manipulation and several more.

. . .

Report details-

19-June-2016—Bug reported to the concerned company.

11-July-2016—Bug was marked fixed.

11-July-2016—Re-tested and confirmed the fix.

1-Aug-2016—Awarded by company.

Thanks for reading!

~Logicbomb (https://twitter.com/logicbomb_1)

Penetration Testing | Ethical Hacking | Bug Bounty | Vulnerability | Hacking

632 claps

2

Avinash Jain (@logicbomb_1)

Lead Infrastructure Security Engineer @groferseng | DevSecops | Part time BugBounty Hunter | Acknowledged by Google, NASA, Yahoo, United Nations, BBC etc.

Follow

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. #sharingiscaring

Follow

More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)

0x0FFB347
Mar 8 · 5 min read
244

More from InfoSec Write-ups

Ping Power—ICMP Tunnel

Nir Chako
Dec 17, 2018 · 8 min re
464

More from InfoSec Write-ups

How to Make a Captive Portal of Death

Trevor Phillips
Dec 18, 2018 · 6 min re
270

Responses

Write a response...

Conversation with Avinash Jain (@logicbomb_1).

Pichaya Morimoto
Mar 4, 2018

You forgot to deduct “payback.in” in the figure before the last one.

1 1 response

Avinash Jain (@logicbomb_1)
Mar 4, 2018

I need to remove this as well. Thanks mate ☺

1

Show all responses