Pwntoken - Digital Security Research

Information Security Sciences with Shritam Bhowmick.

AUG 30TH, 2017 1:00 AM | COMMENTS

Defining an Enterprise Penetration Test

Are Enterprises Aware Of A Defined Penetration Test?

It really took me a complete decade to have a meaningful dedicated routine time having few legit set of questions & debunks we'll be looking at frequencies from here onwards. After having experienced a large number of strategic targets spending a decade of nights, an expensive totalitarian disciplined existence into hacker community circles ranging from the Mexican Boards, Russian Boards to few selected ones for intel since ages now & a sincere Executioner of Myth, Fanatics including an Experience in side swiping Best Charlatans who're evolving at a faster pace;

I have with all such detailed experience in total truth concluded the larger scale enterprises lack a defined understanding of what a **Penetration Test** really is. My study show a very poor performance of the Enterprises at a far capital market reach of a Billion Dollar Industry that the Cyber Security Market can upscale to. I will be the surgeon & would logically be concluding:

Information Security

Shritam Bhowmick
1,227
●11 ●26

Recent Posts

- Defining an Enterprise Penetration Test
- Enterprise Web Application Security Program
- Web Application Security Testing
- Economics of Web Application Security
- Driving-By Dirty Octopress

Top Categories

- web_application_security (3)

1. Are they Aware!?
2. Are Even Cyber Security Companies Themselves Aware?
3. What about the Indian Enterprise Eco-Space - they're looking a complete joke by now.
4. Re-Iterating & Re-Focusing, Do Indian Enterprise Eco-System Aware of a Dis-balanced IT Ops Budget & Security Ops Budget?

.. wait - don't be waiting any longer to have a second thought about mistaking the wide information security domain with just a penetration test. The width I'm talking takes grasping this wide domain .. I'll leave you there to the width in an image below ..

penetration_test (1)

octopress (1)

events (1)

Year Archives

2017

August

Defining An Enterprise Penetration Test

2015

September

Enterprise Web Application Security Program

August

Web Application Security Testing

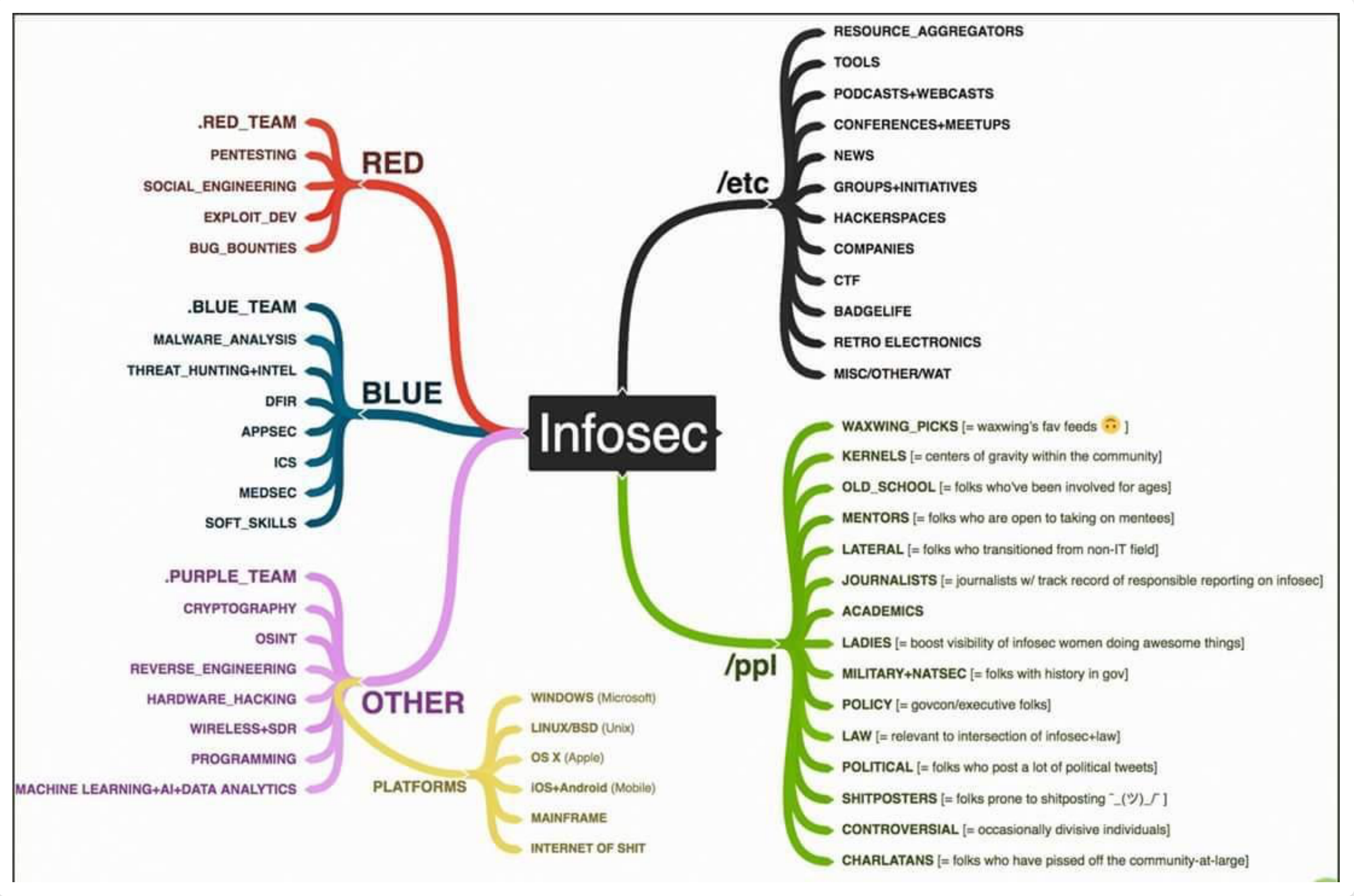
Economics of Web Application Security

July

Driving-By Dirty Octopress

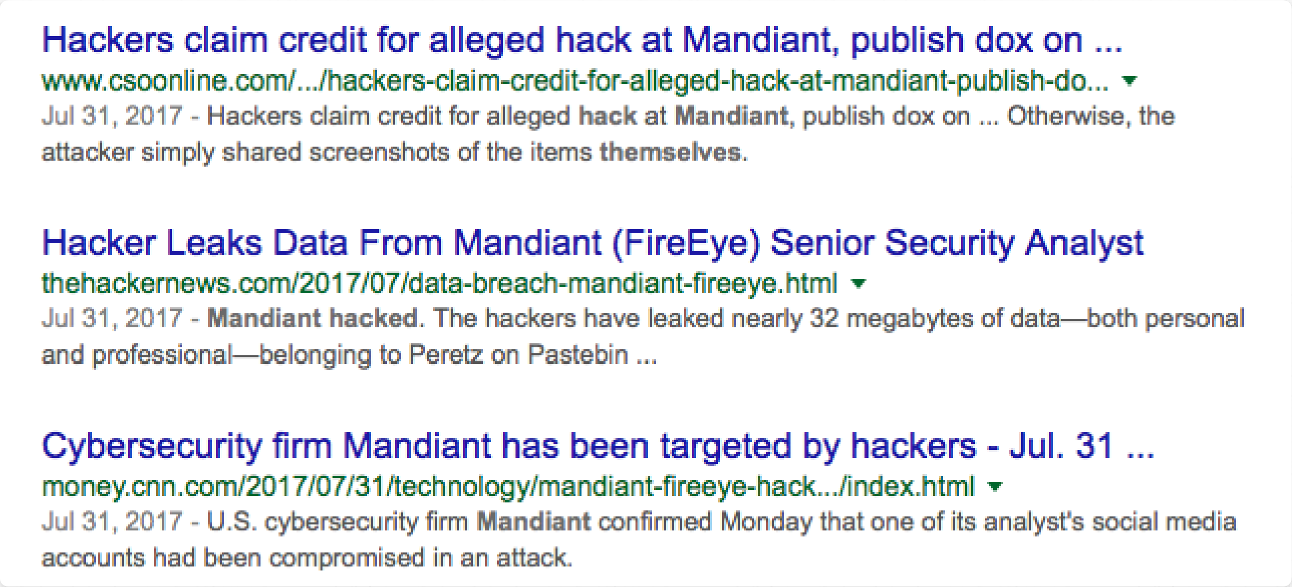
March

Introduction


Infosec
RED
.RED_TEAM
PENTESTING
SOCIAL_ENGINEERING
EXPLOIT_DEV
BUG_BOUNTIES
BLUE
.BLUE_TEAM
MALWARE_ANALYSIS
THREAT_HUNTING+INTEL
DFIR
APPSEC
ICS
MEDSEC
SOFT_SKILLS
OTHER
.PURPLE_TEAM
CRYPTOGRAPHY
OSINT
REVERSE_ENGINEERING
HARDWARE_HACKING
WIRELESS+SDR
PROGRAMMING
MACHINE LEARNING+AI+DATA ANALYTICS
PLATFORMS
WINDOWS (Microsoft)
LINUX/BSD (Unix)
OS X (Apple)
iOS+Android (Mobile)
MAINFRAME
INTERNET OF SHIT
/etc
RESOURCE_AGGREGATORS
TOOLS
PODCASTS+WEBCASTS
CONFERENCES+MEETUPS
NEWS
GROUPS+INITIATIVES
HACKERSPACES
COMPANIES
CTF
BADGELIFE
RETRO ELECTRONICS
MISC/OTHER/WAT
/ppl
WAXWING_PICKS [= waxwing's fav feeds 🙃]
KERNELS [= centers of gravity within the community]
OLD_SCHOOL [= folks who've been involved for ages]
MENTORS [= folks who are open to taking on mentees]
LATERAL [= folks who transitioned from non-IT field]
JOURNALISTS [= journalists w/ track record of responsible reporting on infosec]
ACADEMICS
LADIES [= boost visibility of infosec women doing awesome things]
MILITARY+NATSEC [= folks with history in gov]
POLICY [= govcon/executive folks]
LAW [= relevant to intersection of infosec+law]
POLITICAL [= folks who post a lot of political tweets]
SHITPOSTERS [= folks prone to shitposting ¯_(ツ)_/¯]
CONTROVERSIAL [= occasionally divisive individuals]
CHARLATANS [= folks who have pissed off the community-at-large]

A Penetration Test by any margin among that huge wide Information Security Domain is simply put a task in an organization to settle down on a risk factor which includes live infiltration via the Organization's Asset - the Application Stack or the Network Stack. And no, this doesn't include Social Engineering attack for the `people`, that's `Red Teaming` & has a larger strategical construct. `Red Teaming` includes several other facets & factors involved - We'd debunk that later for good.

Right now, let's focus around `Penetration Test`. What would take an Organization, an Enterprise which is highly decorated in it's all reputed glories from decades of business investments to fall apart from the reputation!? This!



Hackers claim credit for alleged hack at Mandiant, publish dox on ...
www.csoonline.com/.../hackers-claim-credit-for-alleged-hack-at-mandiant-publish-do...
Jul 31, 2017 - Hackers claim credit for alleged **hack** at **Mandiant**, publish dox on ... Otherwise, the attacker simply shared screenshots of the items **themselves**.

Hacker Leaks Data From Mandiant (FireEye) Senior Security Analyst
thehackernews.com/2017/07/data-breach-mandiant-fireeye.html
Jul 31, 2017 - **Mandiant hacked**. The hackers have leaked nearly 32 megabytes of data—both personal and professional—belonging to Peretz on Pastebin ...

Cybersecurity firm Mandiant has been targeted by hackers - Jul. 31 ...
money.cnn.com/2017/07/31/technology/mandiant-fireeye-hack.../index.html
Jul 31, 2017 - U.S. cybersecurity firm **Mandiant** confirmed Monday that one of its analyst's social media accounts had been compromised in an attack.

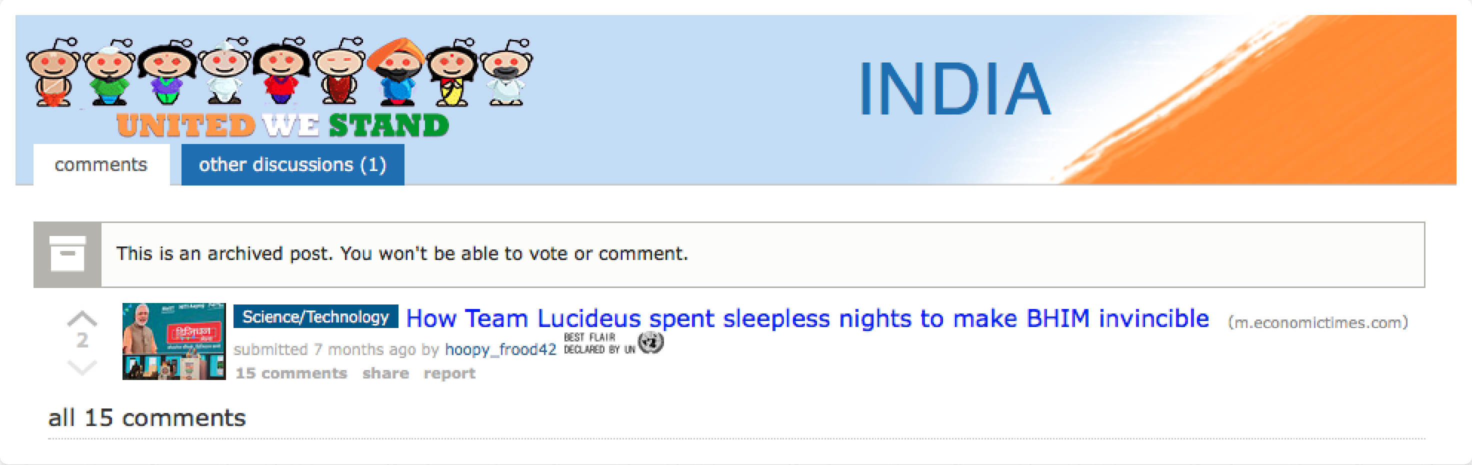
Little to no surprise, The Enterprises are slowly evolving & have introduced `DevOps` which has a more simpler way of an efficient IT Operation but a complex variant of necessary subset & routine security check which's often missed. By this factor, very fewer Organizations have really known the difference between a `Vulnerability Assessment` & a `Penetration Test` given that they understand necessary scopes to be involved.

Given the experiences I had - in my opinion, they **DO NOT YET UNDERSTAND PENETRATION TEST**.

Are Cyber Security Companies Across India Aware?

Whilst being on a standard operation, I had to focus around getting away with analyzing if Claimed Cyber Security Companies are themselves aware. To my amazement - they're completely off that street & have already went boasting their permits without really having any In-Depth measures often to take.

We'll rewind my experience in short & debunk this out since a company called [Lucideus Tech] was recently roasted at Reddit India for the very same reasons. Please don't judge already, I was involved with the operations AVP @ Penetration Testing & resigned due to particularly this nature. Let's take a look at the history how that unfolded ..

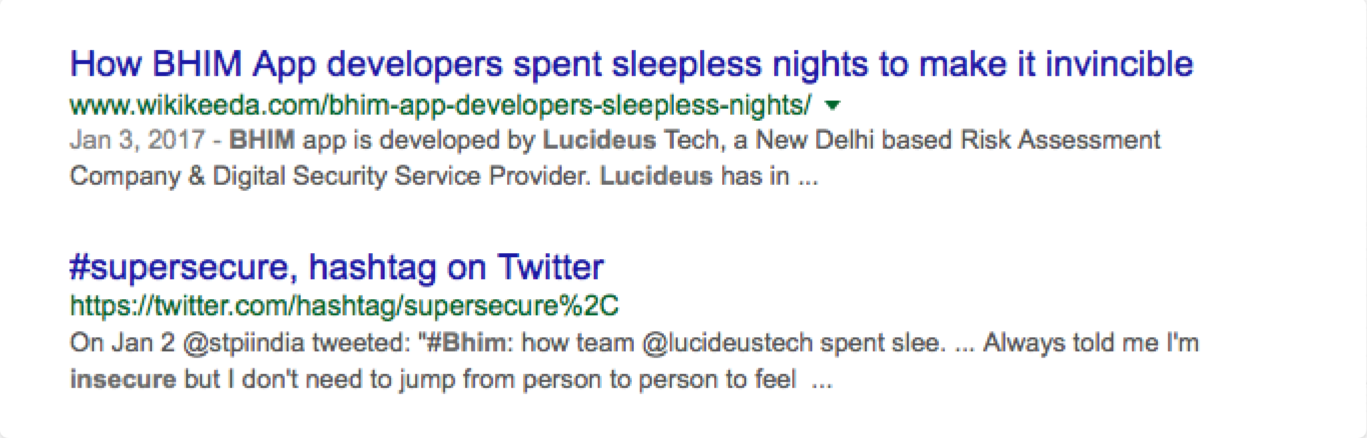


This is an archived post. You won't be able to vote or comment.

Science/Technology How Team Lucideus spent sleepless nights to make BHIM invincible (m.economictimes.com)

submitted 7 months ago by hoopy_frood42

all 15 comments



How BHIM App developers spent sleepless nights to make it invincible
www.wikikeeda.com/bhim-app-developers-sleepless-nights/
Jan 3, 2017 - **BHIM** app is developed by **Lucideus** Tech, a New Delhi based Risk Assessment Company & Digital Security Service Provider. **Lucideus** has in ...

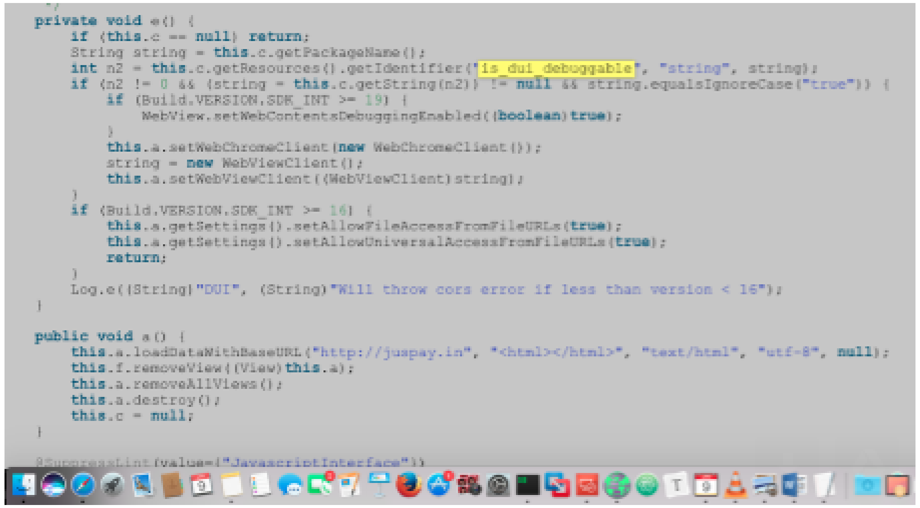
#supersecure, hashtag on Twitter
https://twitter.com/hashtag/supersecure%2C
On Jan 2 @stpiindia tweeted: "**#Bhim**: how team @lucideustech spent slee. ... Always told me I'm **insecure** but I don't need to jump from person to person to feel ...

Looks great, in all format a very better PR team that there is .. In pure amazement, I had to hook up my instruments of mass destructions & concluded it wasn’t really that *secure* as claimed. A complete exchange of the email transcript to me fellow reputed security professionals were as below:

- Failure 1: BHIM lacks functionality tests which means this leverages to a security failure. Technically, the application should not credit & debit to it's own account which it does. This in turn means attackers can cause a service deniable to the server using automated scripts doing this specific operation in a continuous loop.

  Countermeasure: functionality controls to be checked & should be considered one of the unit test gone through in primary development stages

- Failure 2: Code in itself is debuggable which means either the developers or the attackers themselves have access to the source code, which in turn means, from attacker perspective, it's possible to reverse engineer, proof of concept is as below:

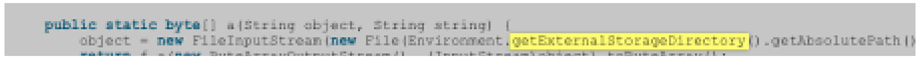


```
    private void e() {
        if (this.c == null) return;
        String string = this.c.getPackageName();
        int n2 = this.c.getResources().getIdentifier("is_dui_debuggable", "string", string);
        if (n2 != 0 && (string = this.c.getString(n2)) != null && string.equalsIgnoreCase("true")) {
            if (Build.VERSION.SDK_INT >= 19) {
                WebView.setWebContentsDebuggingEnabled((boolean)true);
            }
            this.a.setWebChromeClient(new WebChromeClient());
            string = new WebViewClient();
            this.a.setWebViewClient((WebViewClient)string);
        }
        if (Build.VERSION.SDK_INT >= 16) {
            this.a.getSettings().setAllowFileAccessFromFileURLs(true);
            this.a.getSettings().setAllowUniversalAccessFromFileURLs(true);
            return;
        }
        Log.e((String)"DUI", (String)"Will throw cors error if less than version < 16");
    }

    public void a() {
        this.a.loadDataWithBaseURL("http://juspay.in", "<html></html>", "text/html", "utf-8", null);
        this.f.removeView((View)this.a);
        this.a.removeAllViews();
        this.a.destroy();
        this.c = null;
    }

    @SuppressLint(value={"JavascriptInterface"})
```

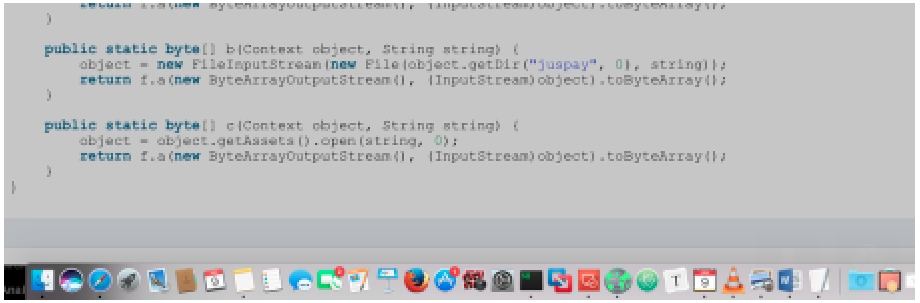
  Countermeasure: Use code obfuscation.

- The BHIM Application allows files to be written in external storage which means, allocation of data on an unsecure external device which could be manipulated later. Proof of concept as below after having revered engineered the code in itself:

- The BHIM Application allows files to be written in external storage which means, allocation of data on an unsecure external device which could be manipulated later. Proof of concept as below after having revered engineered the code in itself:

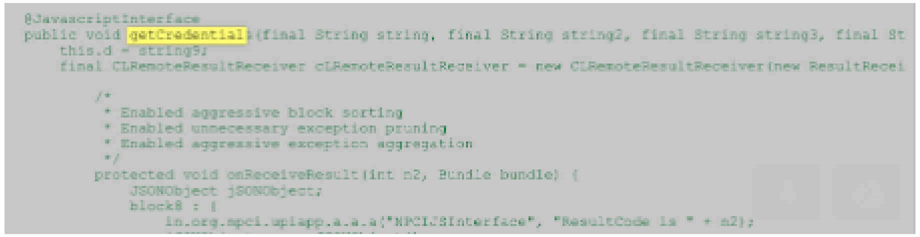


```
    public static byte[] a(String object, String string) {
        object = new FileInputStream(new File(Environment.getExternalStorageDirectory().getAbsolutePath()
```



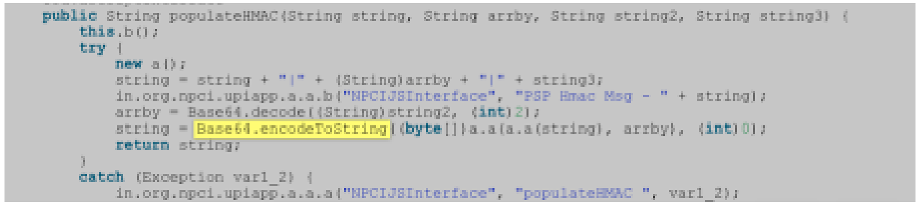
```
        return f.a(new ByteArrayOutputStream(), (InputStream)object).toByteArray();
    }

    public static byte[] b(Context object, String string) {
        object = new FileInputStream(new File(object.getDir("juspay", 0), string));
        return f.a(new ByteArrayOutputStream(), (InputStream)object).toByteArray();
    }

    public static byte[] c(Context object, String string) {
        object = object.getAssets().open(string, 0);
        return f.a(new ByteArrayOutputStream(), (InputStream)object).toByteArray();
    }
}
```

- We were able to complete decode messages from NCPI using weak crypto and basically never having used crypto or otherwise technically called as 'encoders', having said so, we also were able to look through the source code & see implementation details of it:



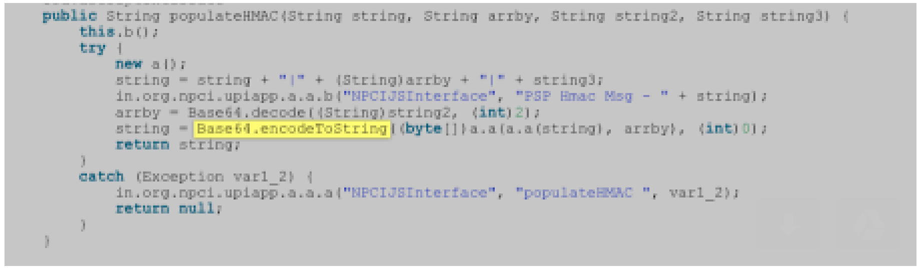
```
@JavascriptInterface
public void getCredentials(final String string, final String string2, final String string3, final St
    this.d = string9;
    final CLRemoteResultReceiver cLRemoteResultReceiver = new CLRemoteResultReceiver(new ResultRecei

        /*
         * Enabled aggressive block sorting
         * Enabled unnecessary exception pruning
         * Enabled aggressive exception aggregation
         */
        protected void onReceiveResult(int n2, Bundle bundle) {
            JSONObject jSONObject;
            block8 : {
                in.org.npci.upiapp.a.a.a("NPCIJSInterface", "ResultCode is " + n2);
```

Here's proof of concept that the NPCI JS module uses Base64 encoders which's not a real crypto at all for credential sharing:



```
    public String populateHMAC(String string, String arrby, String string2, String string3) {
        this.b();
        try {
            new a();
            string = string + "|" + (String)arrby + "|" + string3;
            in.org.npci.upiapp.a.a.b("NPCIJSInterface", "PSP Hmac Msg - " + string);
            arrby = Base64.decode((String)string2, (int)2);
            string = Base64.encodeToString((byte[])a.a(a.a(string), arrby), (int)0);
            return string;
        }
        catch (Exception var1_2) {
            in.org.npci.upiapp.a.a.a("NPCIJSInterface", "populateHMAC ", var1_2);
```

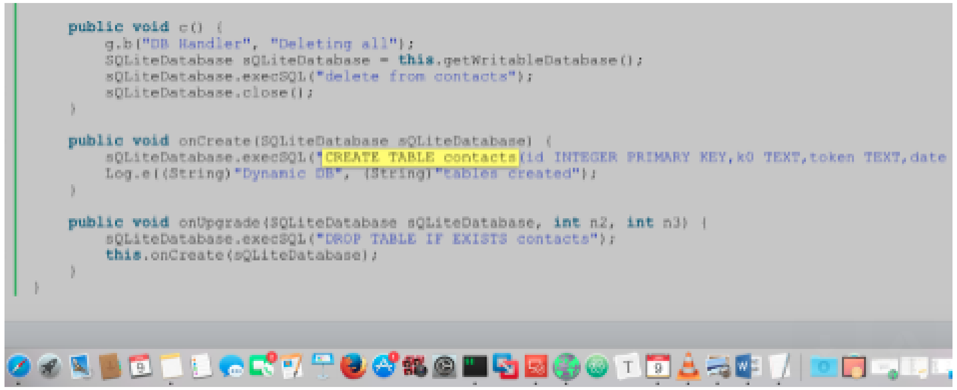
Here's proof of concept that the NPCI JS module uses Base64 encoders which's not a real crypto at all for credential sharing:



```
public String populateHMAC(String string, String arrby, String string2, String string3) {
    this.b();
    try {
        new a();
        string = string + "|" + (String)arrby + "|" + string3;
        in.org.npci.upiapp.a.a.b("NPCIJSInterface", "PSP Hmac Msg - " + string);
        arrby = Base64.decode((String)string2, (int)2);
        string = Base64.encodeToString((byte[])a.a(a.a(string), arrby), (int)0);
        return string;
    }
    catch (Exception var1_2) {
        in.org.npci.upiapp.a.a.a("NPCIJSInterface", "populateHMAC ", var1_2);
        return null;
    }
}
```

Countermeasures: use crypto and not 'encoders'. Encoding & Encryption are both very different concepts.

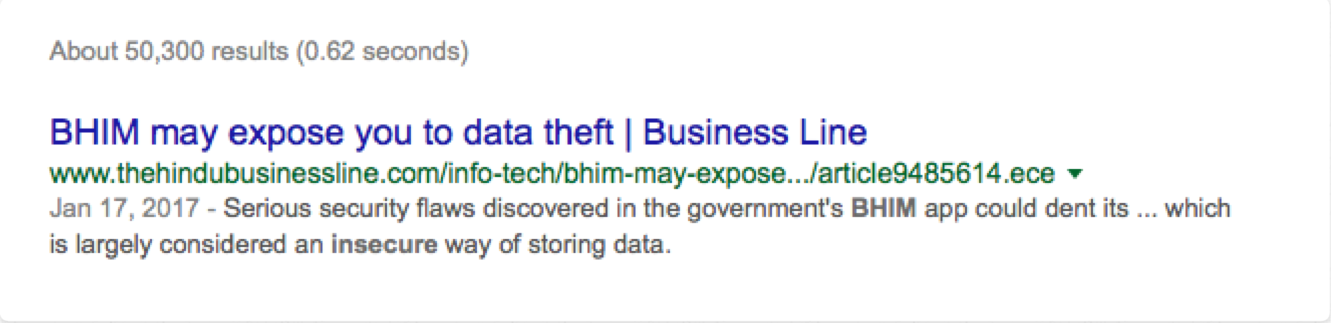
- Next, the database handler in BHIM uses insecure database handling which can often be the cause of unhandled exception; In laymen term - it means exfiltration of user saved data int a database by an attacker; proof of concept is as below:



```
    public void c() {
        g.b("DB Handler", "Deleting all");
        SQLiteDatabase sQLiteDatabase = this.getWritableDatabase();
        sQLiteDatabase.execSQL("delete from contacts");
        sQLiteDatabase.close();
    }

    public void onCreate(SQLiteDatabase sQLiteDatabase) {
        sQLiteDatabase.execSQL("CREATE TABLE contacts(id INTEGER PRIMARY KEY,k0 TEXT,token TEXT,date
        Log.e((String)"Dynamic DB", (String)"tables created");
    }

    public void onUpgrade(SQLiteDatabase sQLiteDatabase, int n2, int n3) {
        sQLiteDatabase.execSQL("DROP TABLE IF EXISTS contacts");
        this.onCreate(sQLiteDatabase);
    }
}
```

Countermeasures: use stored procedures for query calls. Any rooted phones can have the access to the database, there's a risk involved in calling queries from databases without any handled exception procedures.

.. Somehow the Self Claimed Security Pioneers were stupid to not recognize & dared not to take action. On behalf of that, let's un-reveal the truth.



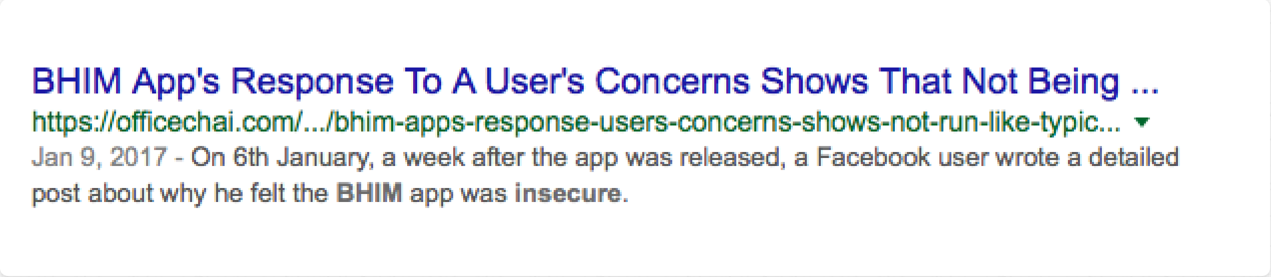
About 50,300 results (0.62 seconds)

BHIM may expose you to data theft | Business Line

www.thehindubusinessline.com/info-tech/bhim-may-expose.../article9485614.ece

Jan 17, 2017 - Serious security flaws discovered in the government's **BHIM** app could dent its ... which is largely considered an **insecure** way of storing data.

The resultant fixes were made & code changes at Android Play Stores were made quickly to compass embarrassment to a direction which were a very generic statement to it’s users.



BHIM App's Response To A User's Concerns Shows That Not Being ...

https://officechai.com/.../bhim-apps-response-users-concerns-shows-not-run-like-typic...

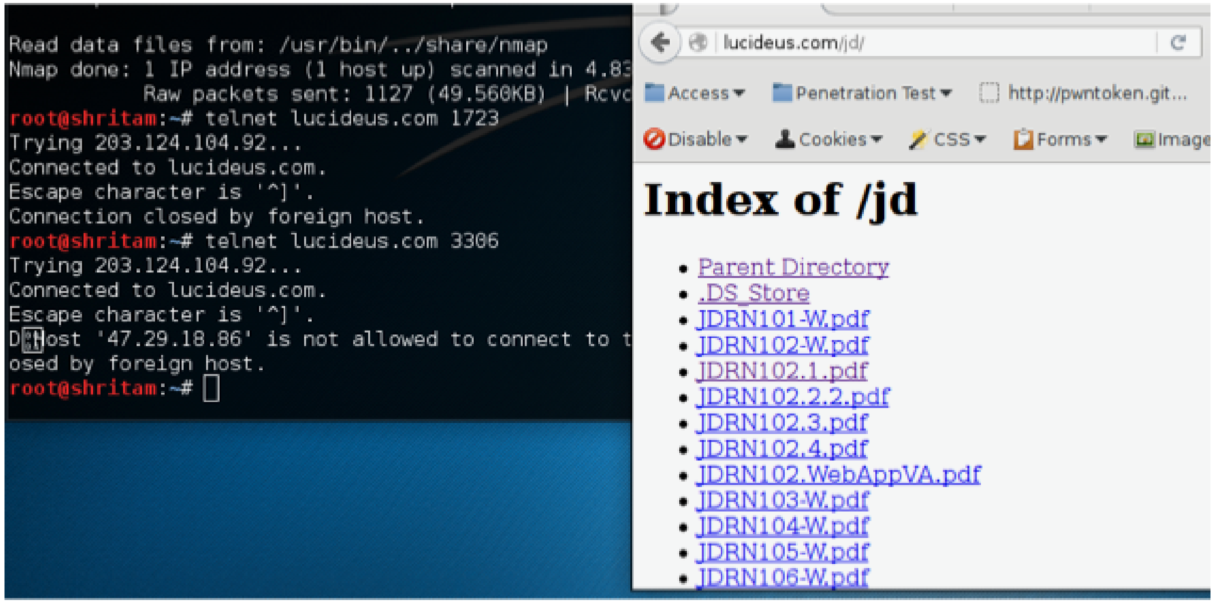
Jan 9, 2017 - On 6th January, a week after the app was released, a Facebook user wrote a detailed post about why he felt the **BHIM** app was **insecure**.

Moving on. I insisted & exchanged couple of mails to Lucideus handler then stating how much such PR doesn’t really help the userbase & insisted on making patches to Lucideus own systems.

Hi Saket,

Hope you're doing well & this mail finds you in great health, It's a pleasure to e-meet you after a long time. We were revising a quick analysis throughout the web presence for Lucideus & found very few information level controls which could be an add to tighten security & could be of value add to Lucideus Integrity (Below are few security controls for the gist of a quick manual security review):

1. A directory listing were found at the /jd/ section:



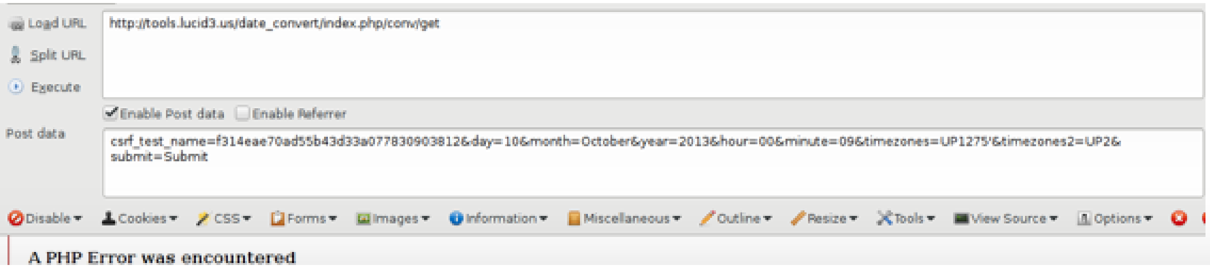
```
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.83
           Raw packets sent: 1127 (49.560KB) | Rcvd
root@shritam:~# telnet lucideus.com 1723
Trying 203.124.104.92...
Connected to lucideus.com.
Escape character is '^]'.
Connection closed by foreign host.
root@shritam:~# telnet lucideus.com 3306
Trying 203.124.104.92...
Connected to lucideus.com.
Escape character is '^]'.
DHost '47.29.18.86' is not allowed to connect to t
osed by foreign host.
root@shritam:~# 
```

lucideus.com/jd/

Index of /jd

- Parent Directory
- .DS_Store
- JDRN101-W.pdf
- JDRN102-W.pdf
- JDRN102.1.pdf
- JDRN102.2.2.pdf
- JDRN102.3.pdf
- JDRN102.4.pdf
- JDRN102.WebAppVA.pdf
- JDRN103-W.pdf
- JDRN104-W.pdf
- JDRN105-W.pdf
- JDRN106-W.pdf

2. An abandoned toolset directory from: http://tools.lucid3.us We noticed a toolset called Time Converter & tried to check if CSRF values were random; They weren't & we tried to manipulate parameters to trigger an error ..



Load URL: http://tools.lucid3.us/date_convert/index.php/conv/get

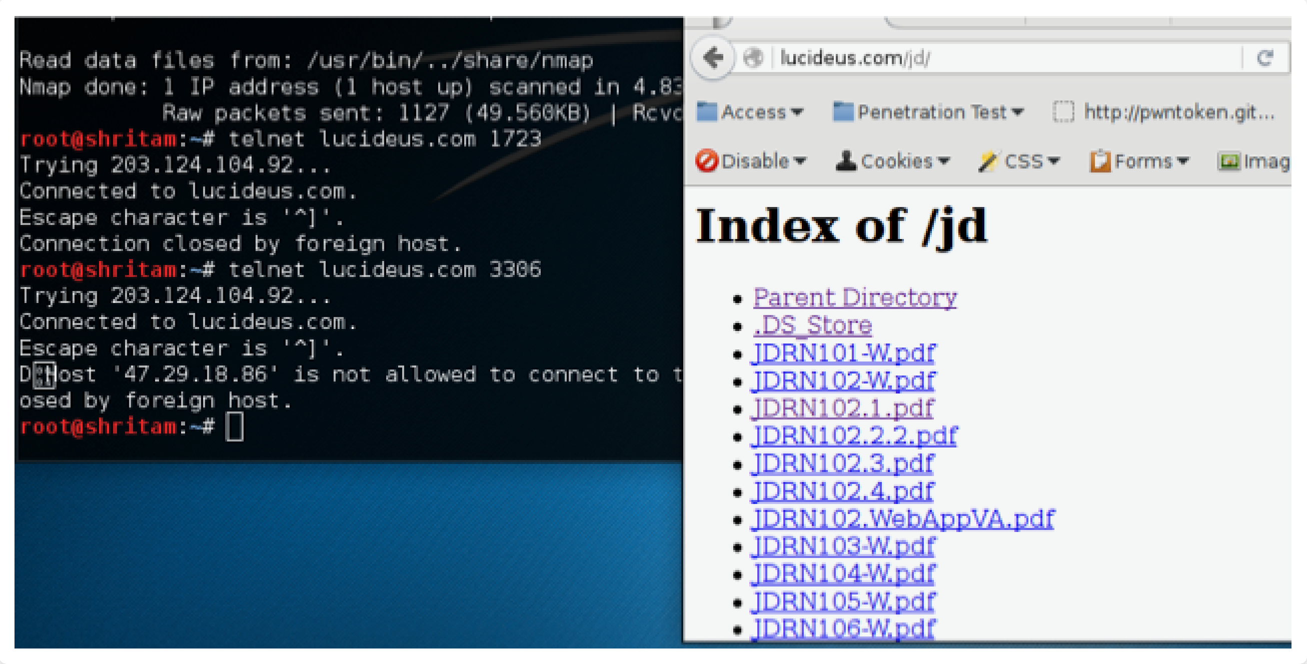
☑ Enable Post data ☐ Enable Referrer

Post data:

```
csrf_test_name=f314eae70ad55b43d33a077830903812&day=10&month=October&year=2013&hour=00&minute=09&timezones=UP1275'&timezones2=UP2&
submit=Submit
```

A PHP Error was encountered

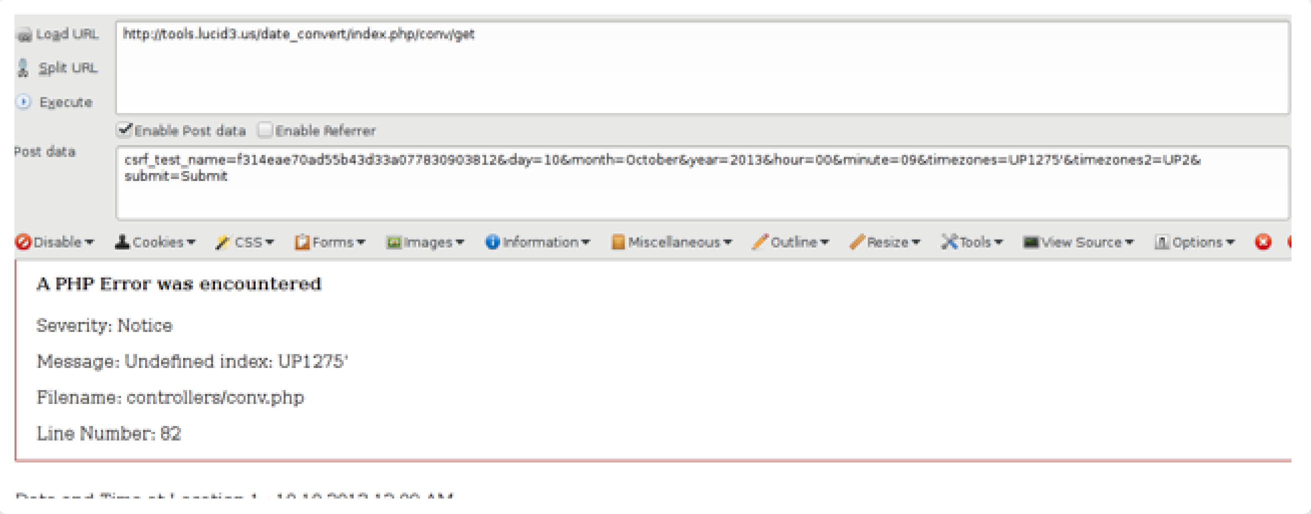
I’d cut this short & re-frame to pointer wise security weaknesses now that the threats are completely patched.



```
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.83
           Raw packets sent: 1127 (49.560KB) | Rcvd
root@shritam:~# telnet lucideus.com 1723
Trying 203.124.104.92...
Connected to lucideus.com.
Escape character is '^]'.
Connection closed by foreign host.
root@shritam:~# telnet lucideus.com 3306
Trying 203.124.104.92...
Connected to lucideus.com.
Escape character is '^]'.
D□Host '47.29.18.86' is not allowed to connect to t
osed by foreign host.
root@shritam:~# 
```

Index of /jd

- Parent Directory
- .DS_Store
- JDRN101-W.pdf
- JDRN102-W.pdf
- JDRN102.1.pdf
- JDRN102.2.2.pdf
- JDRN102.3.pdf
- JDRN102.4.pdf
- JDRN102.WebAppVA.pdf
- JDRN103-W.pdf
- JDRN104-W.pdf
- JDRN105-W.pdf
- JDRN106-W.pdf



http://tools.lucid3.us/date_convert/index.php/conv/get

☑ Enable Post data ☐ Enable Referrer

Post data

```
csrf_test_name=f314eae70ad55b43d33a077830903812&day=10&month=October&year=2013&hour=00&minute=09&timezones=UP1275'&timezones2=UP2&
submit=Submit
```

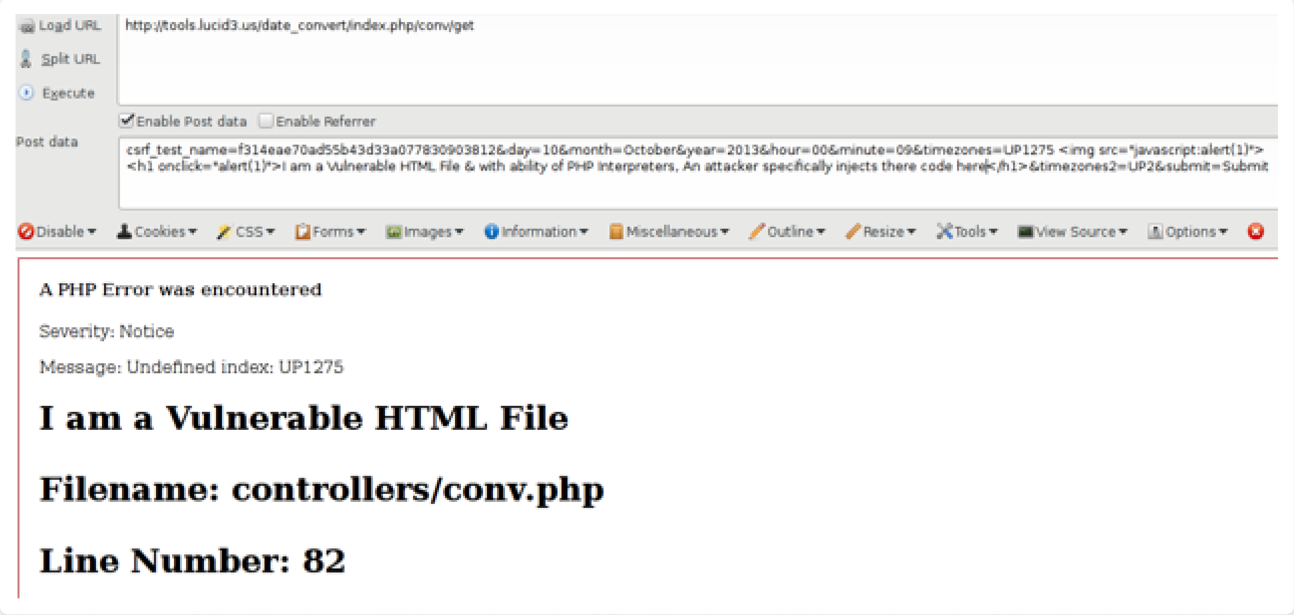
A PHP Error was encountered

Severity: Notice

Message: Undefined index: UP1275'

Filename: controllers/conv.php

Line Number: 82



```
http://tools.lucid3.us/date_convert/index.php/conv/get
```

```
csrf_test_name=f314eae70ad55b43d33a077830903812&day=10&month=October&year=2013&hour=00&minute=09&timezones=UP1275 <img src="javascript:alert(1)">
<h1 onclick="alert(1)">I am a Vulnerable HTML File & with ability of PHP Interpreters, An attacker specifically injects there code here</h1>&timezones2=UP2&submit=Submit
```

A PHP Error was encountered

Severity: Notice

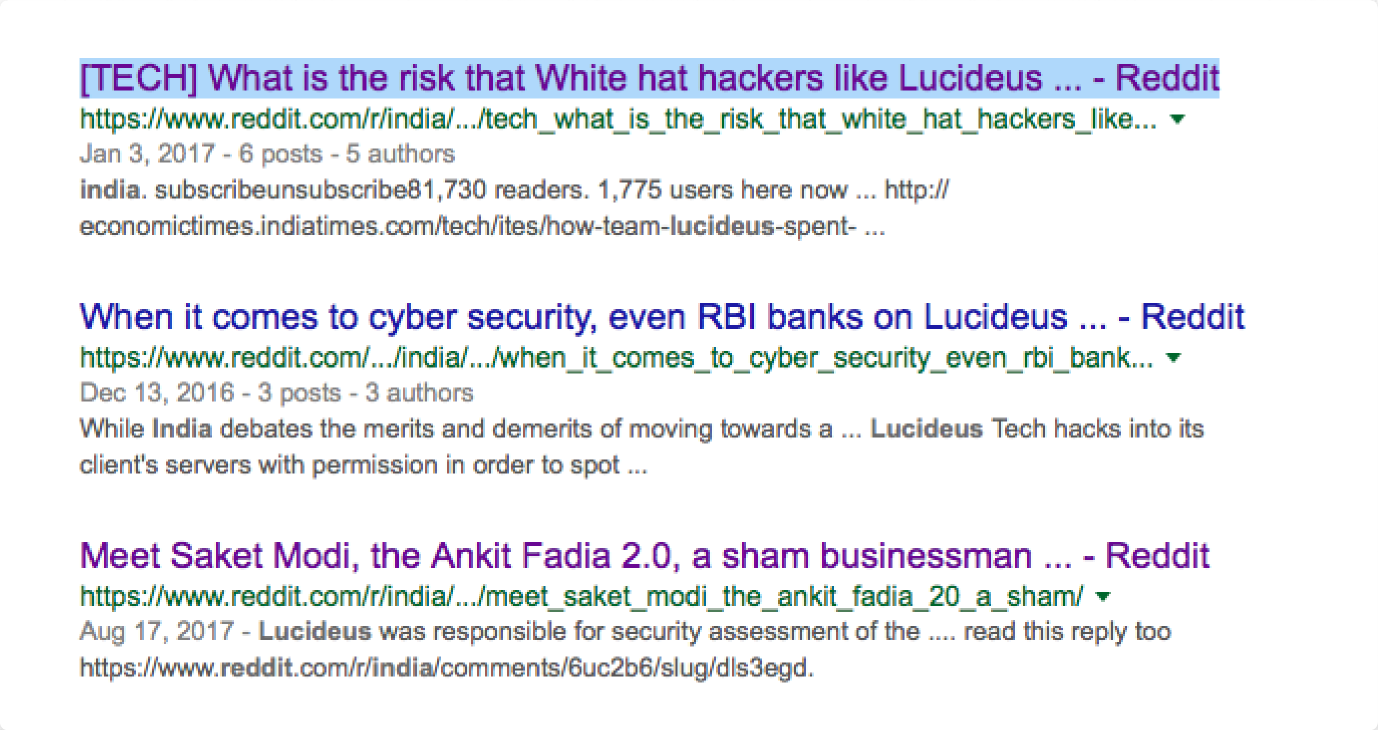
Message: Undefined index: UP1275

I am a Vulnerable HTML File

Filename: controllers/conv.php

Line Number: 82

In short, we're able to trigger JD's & enough PHP mechanisms which could lead to a `Code Injection` variant of an attack. Given that these were patched. We recently now bumped into this below:



[TECH] What is the risk that White hat hackers like Lucideus ... - Reddit
https://www.reddit.com/r/india/.../tech_what_is_the_risk_that_white_hat_hackers_like... ▾
Jan 3, 2017 - 6 posts - 5 authors
india. subscribeunsubscribe81,730 readers. 1,775 users here now ... http://
economictimes.indiatimes.com/tech/ites/how-team-**lucideus**-spent- ...

When it comes to cyber security, even RBI banks on Lucideus ... - Reddit
https://www.reddit.com/.../india/.../when_it_comes_to_cyber_security_even_rbi_bank... ▾
Dec 13, 2016 - 3 posts - 3 authors
While **India** debates the merits and demerits of moving towards a ... **Lucideus** Tech hacks into its client's servers with permission in order to spot ...

Meet Saket Modi, the Ankit Fadia 2.0, a sham businessman ... - Reddit
https://www.reddit.com/r/india/.../meet_saket_modi_the_ankit_fadia_20_a_sham/ ▾
Aug 17, 2017 - **Lucideus** was responsible for security assessment of the .... read this reply too https://www.**reddit**.com/r/**india**/comments/6uc2b6/slug/dls3egd.

comments | other discussions (1)

126

Non-Political Meet Saket Modi, the Ankit Fadia 2.0, a sham businessman masquerading as a hacker. (self.india)
submitted 12 days ago * by NotTheBeliever 2 + 2 = 4?

https://youtu.be/smt8tuNpToM

That's a recent talk he gave, where he makes all kinds of ridiculous claims. He claims to have hacked a phone with 20-30 seconds of physical access to a phone. Then he goes on to show call logs, sms etc etc. Doesn't explain how he does any of that.

Well, he kinda did explain it 3 years ago though, at TEDx conference where he was discussing privacy concerns, now he is a businessman.

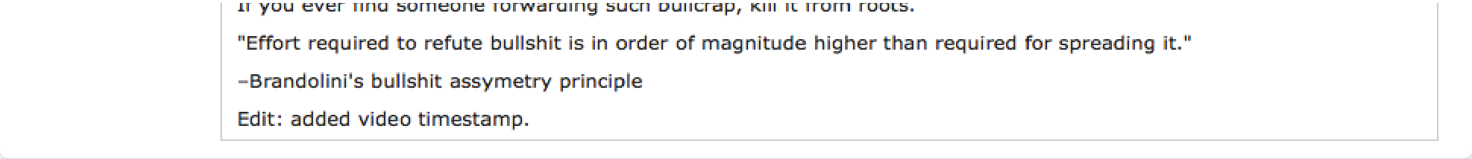
Edit: https://youtu.be/8JED9JDMhzo?t=252

Turns out he installed an app and granted all permissions. He admits to that in old TEDx video but doesn't care to mention it now, because fuck technology, I am here for muh monies. (4:20 in TED video.)

To top it all off, he claims that whatsapp encryption is broken and they fix it every two weeks, "it's a cat and mouse game".

Worst takeaway from all this? People believe him, corporates believe him, his business runs well.

If you ever find someone forwarding such bullcrap, kill it from roots.



If you ever find someone forwarding such bullcrap, kill it from roots.

"Effort required to refute bullshit is in order of magnitude higher than required for spreading it."

–Brandolini's bullshit assymetry principle

Edit: added video timestamp.

It concludes two take-away morales:

- PR does make a Cyber Security Company Glitter.
- PR somehow doesn't make their end users secure.

This additionally concludes our question **"Are Indian Cyber Security Companies Aware?"**, Be my guest to be the judge.

..Mmmhm And What About the Indian Eco-Space Enterprises?

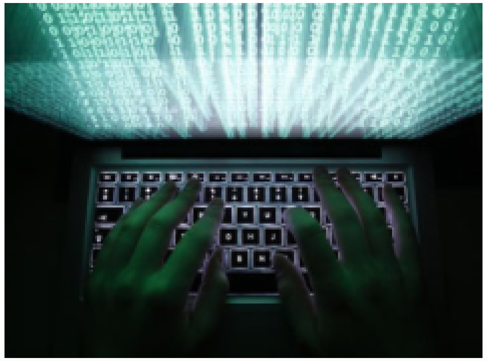
Now that pretty cosmetics are really well priced. Please know, compliances in Security are easy earned certificates but definitely a hard earned cash equaling to business risks for any investment banks or the investors & cannot already be managed fruitfully if left to BugBounty Programs. I'd debunk that later, but hey!

RedBus confirms hack, says no sign of user passwords being stolen yet

The company has asked customers to reset their passwords as a precaution

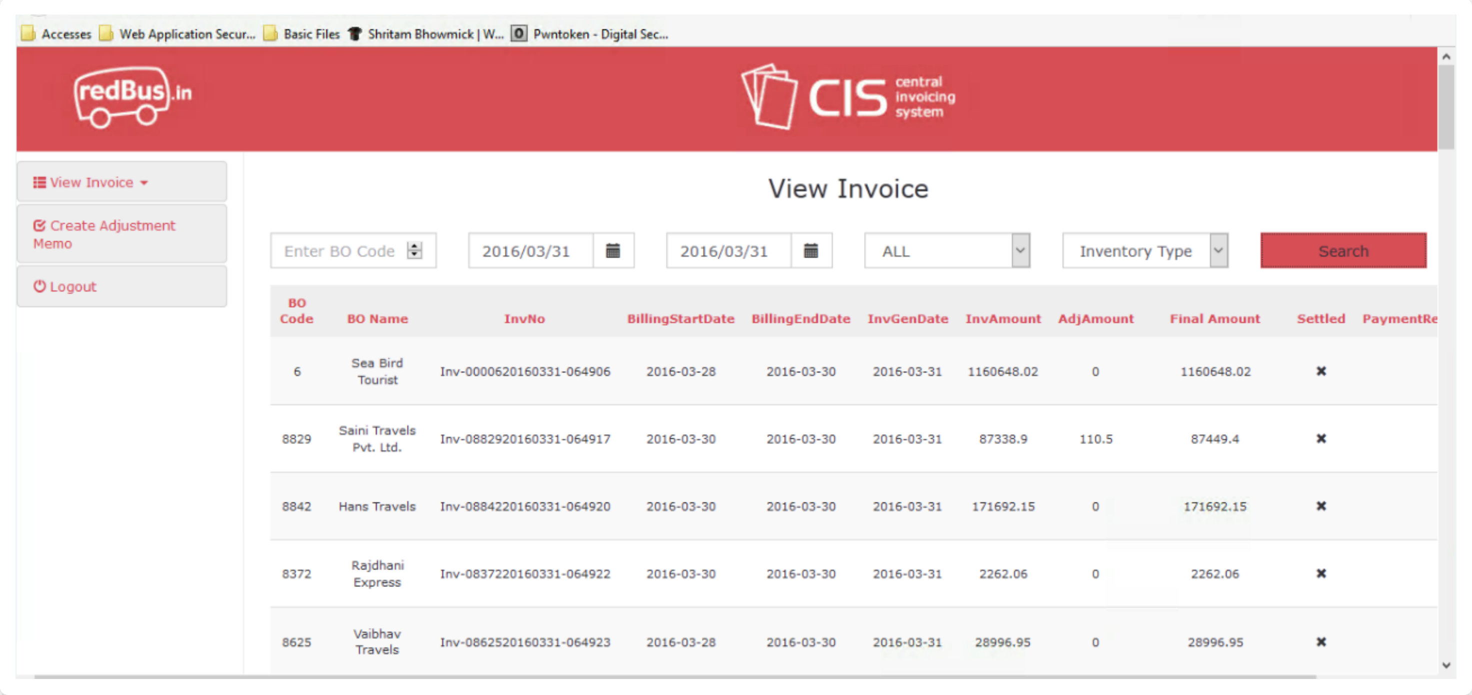
Alnoor Peermohamed | Bengaluru
Last Updated at October 18, 2016 20:32 IST

22 20 4



Online travel giant ibibo Group-owned

No! Invoices were!



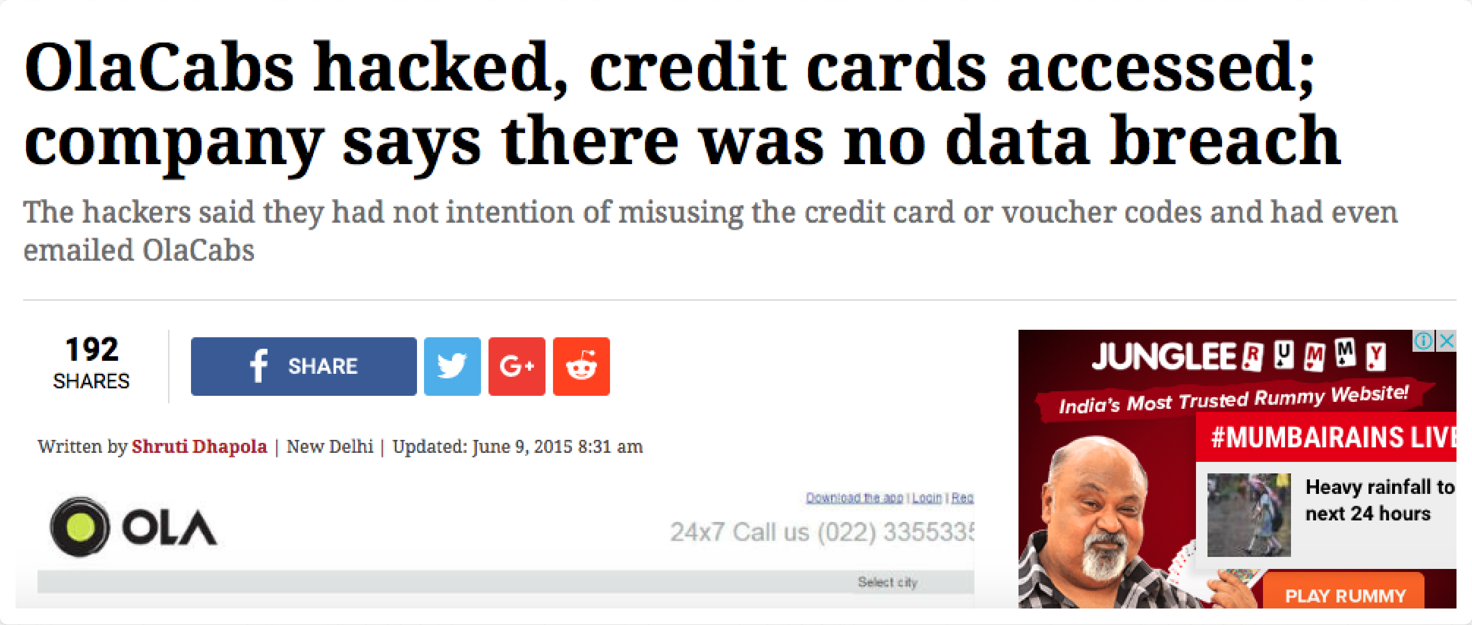
View Invoice

2016/03/31 | 2016/03/31 | ALL | Inventory Type

BO Code	BO Name	InvNo	BillingStartDate	BillingEndDate	InvGenDate	InvAmount	AdjAmount	Final Amount	Settled	PaymentRe
6	Sea Bird Tourist	Inv-000620160331-064906	2016-03-28	2016-03-30	2016-03-31	1160648.02	0	1160648.02	✖	
8829	Saini Travels Pvt. Ltd.	Inv-0882920160331-064917	2016-03-30	2016-03-30	2016-03-31	87338.9	110.5	87449.4	✖	
8842	Hans Travels	Inv-0884220160331-064920	2016-03-30	2016-03-30	2016-03-31	171692.15	0	171692.15	✖	
8372	Rajdhani Express	Inv-0837220160331-064922	2016-03-30	2016-03-30	2016-03-31	2262.06	0	2262.06	✖	
8625	Vaibhav Travels	Inv-0862520160331-064923	2016-03-28	2016-03-30	2016-03-31	28996.95	0	28996.95	✖	

The patch has been responsibly taken care of by now. It's to bring the essence of where the Indian Enterprises are failing. To opt another example out as per Public Disclosure Record after Glorious Patch Success Days ..

.. This was exactly what needs to be pointed out in the Indian Eco-System, you really do not need to articulate non-closures if not already taking Security Operations Serious, more explanation to that later in this series ..



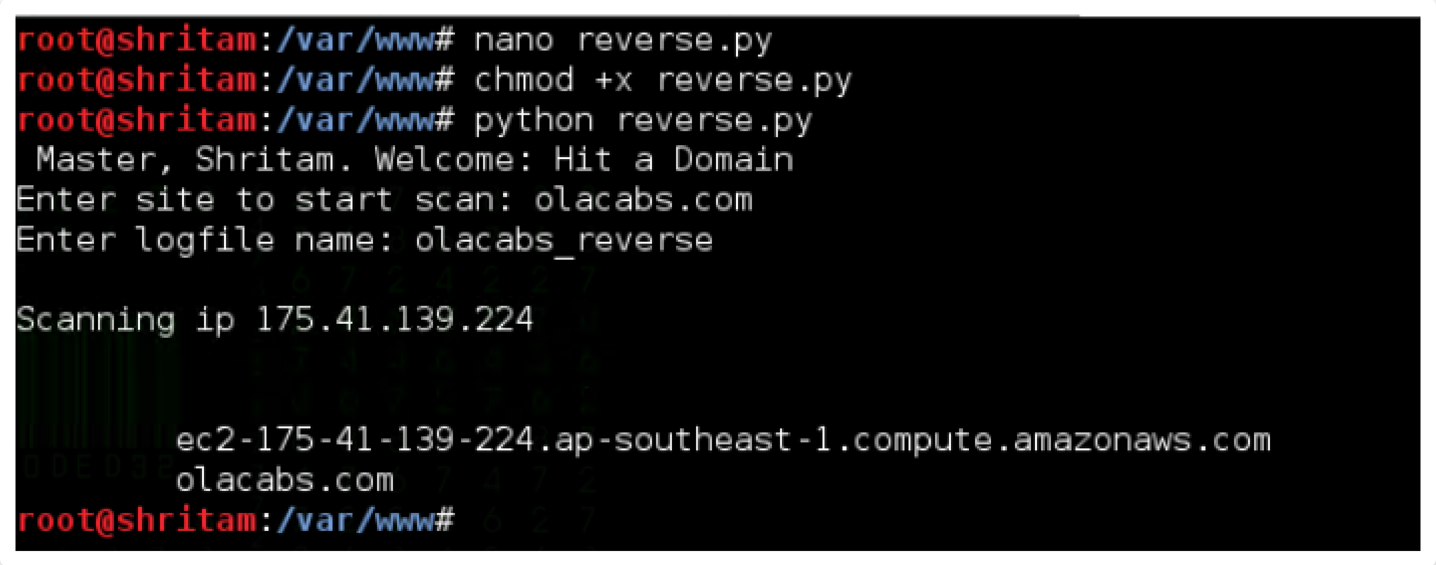
OlaCabs hacked, credit cards accessed; company says there was no data breach

The hackers said they had not intention of misusing the credit card or voucher codes and had even emailed OlaCabs

192 SHARES

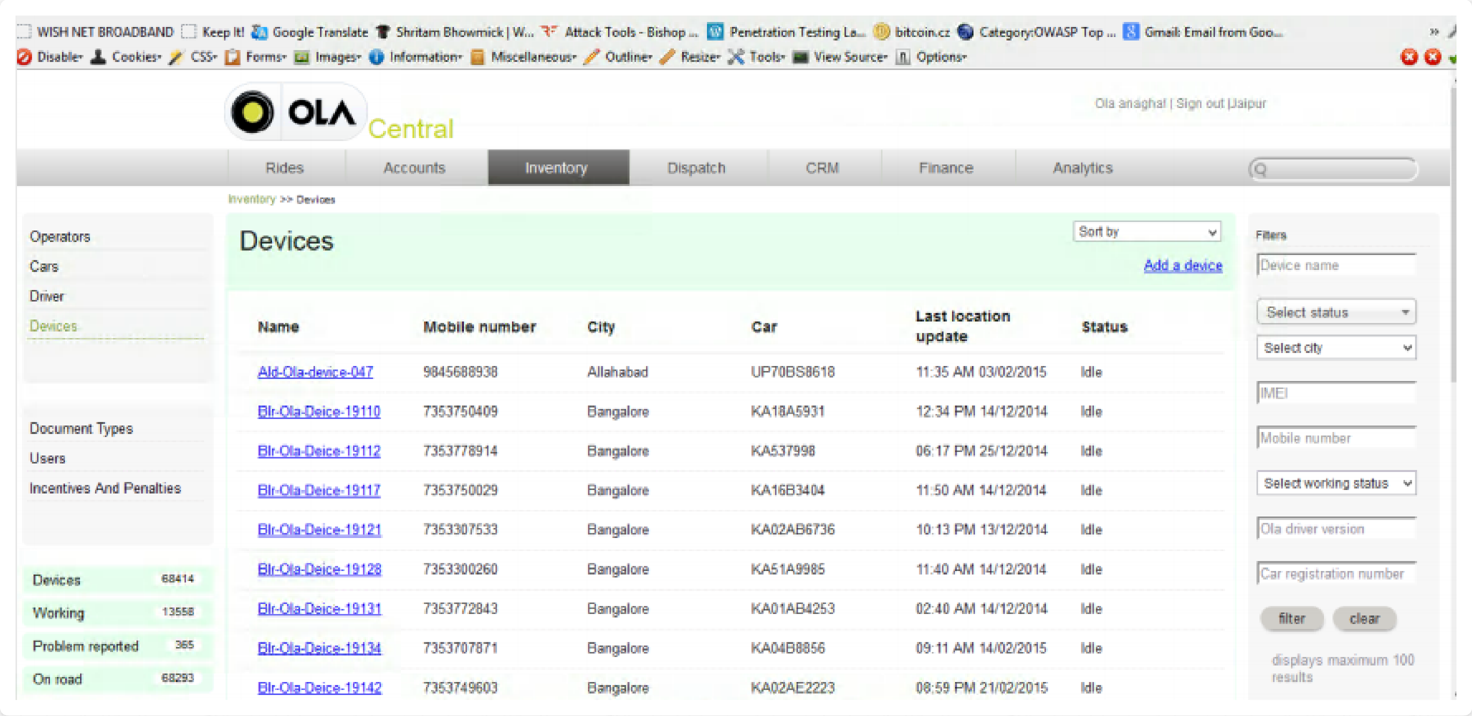
Written by Shruti Dhapola | New Delhi | Updated: June 9, 2015 8:31 am

Amazon Servers are real taste these days ..



```
root@shritam:/var/www# nano reverse.py
root@shritam:/var/www# chmod +x reverse.py
root@shritam:/var/www# python reverse.py
 Master, Shritam. Welcome: Hit a Domain
Enter site to start scan: olacabs.com
Enter logfile name: olacabs_reverse

Scanning ip 175.41.139.224


        ec2-175-41-139-224.ap-southeast-1.compute.amazonaws.com
        olacabs.com
root@shritam:/var/www#
```

.. Sad proved to be very misleading story.



Devices

Name	Mobile number	City	Car	Last location update	Status
Ald-Ola-device-047	9845688938	Allahabad	UP70BS8618	11:35 AM 03/02/2015	Idle
Blr-Ola-Deice-19110	7353750409	Bangalore	KA18A5931	12:34 PM 14/12/2014	Idle
Blr-Ola-Deice-19112	7353778914	Bangalore	KA537998	06:17 PM 25/12/2014	Idle
Blr-Ola-Deice-19117	7353750029	Bangalore	KA16B3404	11:50 AM 14/12/2014	Idle
Blr-Ola-Deice-19121	7353307533	Bangalore	KA02AB6736	10:13 PM 13/12/2014	Idle
Blr-Ola-Deice-19128	7353300260	Bangalore	KA51A9985	11:40 AM 14/12/2014	Idle
Blr-Ola-Deice-19131	7353772843	Bangalore	KA01AB4253	02:40 AM 14/12/2014	Idle
Blr-Ola-Deice-19134	7353707871	Bangalore	KA04B8856	09:11 AM 14/02/2015	Idle
Blr-Ola-Deice-19142	7353749603	Bangalore	KA02AE2223	08:59 PM 21/02/2015	Idle

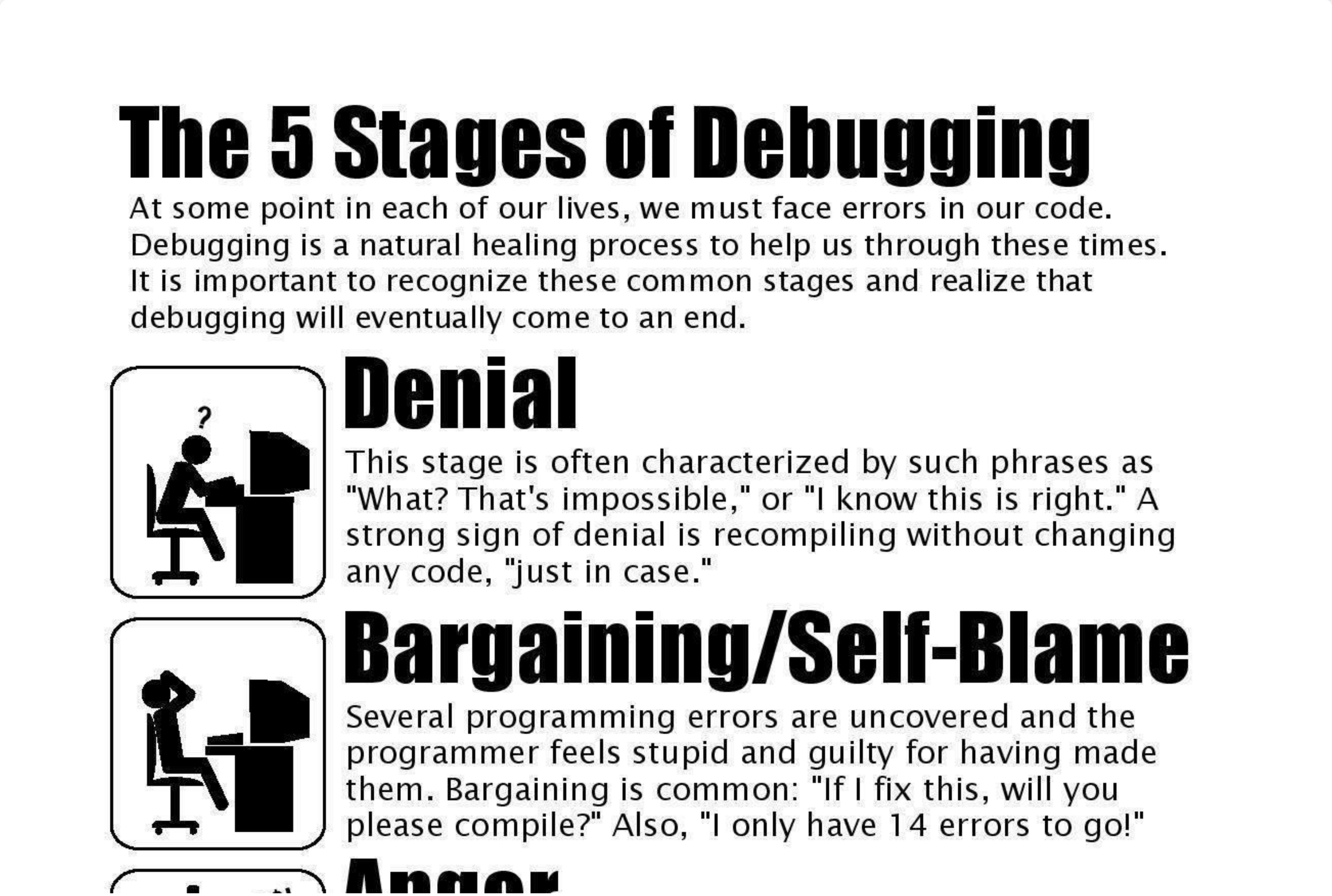
Devices	68414
Working	13558
Problem reported	365
On road	68293

All patches were responsibly closed. This isn’t about the de-motivation but to really take a point across - BugBounties often isn’t any real Penetration Testing to start with nor a Vulnerability Assessment can make organizations any better. The Indian Eco-System has sustained by the rule of Politics where it bends the way management decides but this only later proves the fish to be roasted later during serious compliances & disclosures.

Hence, point proved to our questioning of **Does Indian Enterprise Eco-Space take Security Operations Serious?**. Please be my Guest to be the Judge. The Executioner & this to me, atleast is looking like a complete Joke by now. This isn’t about these Enterprises - ALL of them have a positive hit ratio. Let’s not try turning a Blind Eye!

Let’s Re-Focus Ourselves to the Cause & Countermeasures!

- Blame Game
- Poor Work Culture
- Management Politics Dependency
- .. & etc ..



The 5 Stages of Debugging

At some point in each of our lives, we must face errors in our code. Debugging is a natural healing process to help us through these times. It is important to recognize these common stages and realize that debugging will eventually come to an end.

Denial

This stage is often characterized by such phrases as "What? That's impossible," or "I know this is right." A strong sign of denial is recompiling without changing any code, "just in case."

Bargaining/Self-Blame

Several programming errors are uncovered and the programmer feels stupid and guilty for having made them. Bargaining is common: "If I fix this, will you please compile?" Also, "I only have 14 errors to go!"

Anger

Anger

Cryptic error messages send the programmer into a rage. This stage is accompanied by an hours-long and profanity-filled diatribe about the limitations of the language directed at whomever will listen.

Depression

Following the outburst, the programmer becomes aware that hours have gone by unproductively and there is still no solution in sight. The programmer becomes listless. Posture often deteriorates.

Acceptance

The programmer finally accepts the situation, declares the bug a "feature", and goes to play some Quake.

Most Organizations do not have a well defined IT Operations & IT Security Operations Segregation ..

1. You heard it. The processes itself which segregates IT Security Operations from that of normal IT Operations aren’t segregated & eventually run parallel thinking **buying a really costly https certificate would help prevent any & every attacks**.

2. There are **no ways to communicate to upper management on a defined segregation of IT Operations Budget to that of IT Security Operations Budget** which entirely at a later stage put the Organization to the every possible Security Risk in-front of their investors. This really is a problem when you do not have an approved budget for any expenditure on Security lest the whole hard work in already in ruins.

3. Organization Managers are not well informed of their IT Operations Risks & Hazards as this will definitely put senior managers to an extra work load & few might even miss a beautifully love wedding at Miami Beach for that matter. Most **managers, senior managers cum Executive Directors including that of Excreting on Money Current Chairmen & the Board Of Directors DO NOT UNDERSTAND Security Risks, Threats, Glitches & eventually everything that's in-between.**

Organizations literally BUY Compliances without really any Actual Compliance ..

1. **Buy a https certificate & they'll say you're secure.** Please re-consider, you're just not.

2. **Get a fancy Compliance Security Audit done from a Big4 & you're Secure?**: I've gotten this really covered & laughed ~~twice~~ thrice to this. I'd only hint all Big4's at this moment compromised.

3. **They trust Certificates**: when hiring, this really doesn't work for Security Operations bench. EC|CEH certified will be really a waste for your resource. Use money & use a brain!

The Trendy Bug Bounty get's the Cut!?

Just don't. You'll realize when I make this post useful & define penetration tests at later stages & it's applicable scopes for different ranges of selected optimized on a very controlled productivity-full for maximizing end-results with different unique modes in SecOps (Security Operations).

I intend to Debunk Bug Bounties at a later part in my life time in order to save me the disaster of just proving as it is meant to be proved in true fashion. I'm hoping my readers can direct me to a great gentlemen who can take this up for me using the mainstream media houses.

When it's Pricey?

1. When Organizations are literally bombarded with a FULL DISCLOSURE which evaporates money, finances, data, reputation & probably would risk their wives if lucky in the sleepless process.

2. When Organizations are dis-qualified to be any more Compliant to that Investment Bank you're hoping not checking in security controls. Better Stay non-compliant if not ready. Because it's just a major embarrassment.

3. When userbase have alternatives & they really think their data isn't any safe than the duck aimed to be killed & not even pyre/burial arrangements are made.

4. When Organizations are ransomed. But instead later, kicked again after having the ransom money. haha. That was humorous tho. That's called the state of getting into a `over pricey` tricky situation in the White House Situation Room during an Afgan War lost because Special Forces were not given real equipments for the war operations.

Posted by Shritam Bhowmick • Aug 30th, 2017 1:00 am • penetration_test

Tweet Like Share Sign Up to see what your friends like.

Hello. Welcome to pwntoken. Shritam is an Information Security Analyst cum Penetration Tester. He does Application Security and here's his LinkedIn for a professional touch. Feel free to discuss about the post content and you can send him f eedbacks, if any, at his email (✉).

Follow @pwntoken

« Enterprise Web Application Security Program

Comments

1 Comment Pwntoken 1 Login

♡ Recommend Tweet Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Abhishek sharma • 10 months ago

Great post bro...

Reply • Share ›

Subscribe Add Disqus to your site Disqus' Privacy Policy DISQUS