Bug Bounty Programs Evolution
Zombies!!!
Defacement
OPEN SOURCE

AntiDef Secure TDD

Memory Scraper
Research Bug Bounty Programs Since 2011
If you can’t beat them, join them!
Not cost-effective

Virtual Environment + Bounty Hunter ≠ Safe Bug Bounty Program
Ideas worth spreading
The Evolution
Bounty Hunters in Real Life
First to say that this is serious, it is not a joke. If you ask yourself why someone would need to hire hitman online, I will tell you simply: because it is anonymous. You can always find examples of criminals who collaborated with cops when they face 20 years of prison, and you can finish in the prison because of that. At other side, you can always find examples that police found who had interest to kill dead person and they can come to you and you can give testimony and hitman can finish in the prison 20 years. So, it is mutual interest to make everything anonymously.

This website is hosted at anonymous server, server access to Internet through Tor network, you can access this site anonymously only through Tor network, and I uploaded files to server through Tor network. You make payment with anonymous digital currency called Bitcoin (currently 1 Bitcoin worth about 7 EUR). It means I don't know you and you don't know me. I can't send you in the prison and you can't send me in the prison. Of course you must take a risk when you pay in advance, but there is no interest and profit without risk. You take risk and when you do it anywhere, someone can always cheat you and as I said, many criminals have balls to do many things to the other people but when their ass face 20 years of prison they begin to talk with police. Risk about prison and money is always present. If you are not ready to take a risk, don't contact me. Prices below are in EUR but EUR is facing crisis, so, you should count gold converted in Bitcoins. 5000 EUR is 120gr of gold, 10000 EUR is 240gr of gold and so on. One gram of gold has value of 41,73 EUR or 52,83 US Dollars.
Successful Kill $
Successful Kill = Good Reputation
Targets

Animals  VIP
Politicians  Women
Kids  Men
Hit men
1st Bug Bounty Program
“...REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE”
How did it work?
Winners Awards
Success || Failure

Story?
Firefox developer builds ("Nightly") are now using a new certificate verification library we’ve been working on for some time, and this code is on track to be released as part of Firefox 31 in July. As we’ve all been painfully reminded recently (Heartbleed, #gotofail) correct code in TLS libraries is crucial in today’s Internet and we want to make sure this code is rock solid before it ships to millions of Firefox users. To that end we’re excited to launch a special Security Bug Bounty program that will pay $10,000 for critical security flaws found and reported in this new code before the end of June.
Perspectives on Bug Bounty Programs
Start Your Own Online Program

Technology
Operations
Legal
Start Your Own Online Program

Handle heavy traffic

Technology
Start Your Own Online Program

Technology

Stronger IPS
Start Your Own Online Program

Technology

Stronger WAF
Start Your Own Online Program

Incident Response

Operations

Bugs Management
Start Your Own Online Program

Liability

ENTER AT YOUR OWN RISK

Legal
Identity Verification

External
Post it Here!

External
Traffic Shaping External
Payment Models
Real-World Hacking Scenario
Security Leader Positioning
Sensitive Data Leakage
Denial of Service
Black Hats Detection
## Detailed Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full title</strong></td>
<td>Facebook - Delete The Admin Of Any Page Exploit</td>
</tr>
<tr>
<td><strong>Date add</strong></td>
<td>2013-12-23</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>web applications</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>tricks</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>It is possible to delete the admin of any page just with a single click. This can also be converted into a bot or a worm leading to the deletion of admin of thousands of pages. It is also possible to fully automate this worm. It is very effective when we aim for wide spread attack. Targeted attacks are also possible. This bug is not available public. This bug is tested against hundred's for pages and is found working 100%.</td>
</tr>
<tr>
<td><strong>Usage info</strong></td>
<td>I have automated all the process. Buy it and i will send it. Very simple to use.</td>
</tr>
<tr>
<td><strong>Tested on</strong></td>
<td>Main Website Of Facebook</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>Not Yet Fixed By The Facebook Security Team</td>
</tr>
<tr>
<td><strong>Tags</strong></td>
<td>Facebook zero Dec 2013 Deletion of admin of any page UNPATCHED.</td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>17</td>
</tr>
<tr>
<td><strong>Views</strong></td>
<td>37958</td>
</tr>
</tbody>
</table>
Non-security Bugs Handling
Side Effects

Hello Hero

We have noticed the Bsta027 target, [Redacted], is experiencing severely degraded performance.

Please limit automated scanning to a bare minimum or not at all.

Thank you

The Bugcrowd Team
Minimize Exposure Time
Perspectives on Bug Bounty Programs
Experienced Researchers
Motivation
Frustration
Denial of service

Nir Valtman
Hello, We would like to report about a denial of service exploit on mobile ap...

9/24/13

product-security@[redacted].com
Please include the line below in follow-up emails for this request. Follow-up...

9/26/13

Nir Valtman
Follow-up: [redacted] Hello, Have you managed to fix this exploit? Thanks, Nir

10/7/13

product-security@[redacted].com <product-security@[redacted].com> to me

Please include the line below in follow-up emails for this request.

Follow-up: [redacted]

Hello Nir,

In order to help us reproduce and investigate this issue, we will need some additional details. Can you please send us a the [redacted]

Best regards,
Brandon
Product Security

10/9/13
Changes to Program Terms

The Bug Bounty Program is subject to change or cancellation by PayPal at any time, without notice. As such, PayPal may amend these Program Terms at any time by posting a revised version on our website. By continuing to participate in the Bug Bounty Program after PayPal posts any such changes, you accept the Program Terms, as modified.
Case Study
Name: Oren Hafif
Source: www.orenh.com

Actual Risk
Exposing all hosted email addresses in Google

1st Response
DENIED!

2nd Response
$500 Reward
Next Generation Bug Bounty Programs
Minimize Production Risks
Minimize Production Risks

Allow Penetration Tests

Prevent Malicious Exploitation
Minimize Production Risks

- mobile app
- website
- web service

WWW

4580...

1J8HK7B
Congratulations!

You found sensitive data on the tested application.

Please copy the following token to the new bug page and fill the required fields.

Your token is [Token]

If you have any questions or comments, please let us know using the contact us form.

Have a nice bug bounty hunting,
Crowdome team
Minimize Production Risks
Minimize Production Risks
Minimize Production Risks

Diagram showing cloud services connected to a mobile app, web site, and web service.
Minimize Production Risks
HOW TO IDENTIFY BLACK HAT HACKERS?
LEGITIMATE SQL INJECTION

`' or 'a'<'b';#
SELECT 0x457578

MALICIOUS SQL INJECTION

DROP myTable;#
DR/**/OP/*bypassing filter*/myTable;#
SELECT LOAD_FILE(0x633A5C626F6F742E696E69)
HOW TO BAN THEM?
ATTRACT NEW TESTER TYPES

- Business Analysts
- Attorneys
- Developers
- SME
- Quality Assurance
A LONG JOURNEY IN FRONT OF US
Thank You