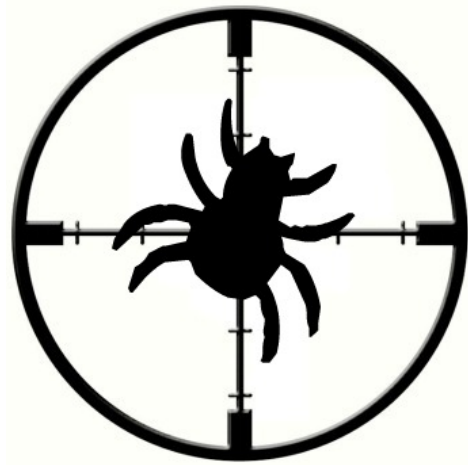


Bug Bounties

Cén scéal?



What do I do?

- Freelance Security Consulting
- Bug Bounties
- Security Research
- Recently signed as a contracted remote Application Security Engineer with **bugcrowd**

Who am I?

Ciarán McNally



Why Care?

- Top 50 on two of the worlds largest Responsible Disclosure Platforms.

ciaran@securit.ie

www.securit.ie

twitter.com/@ciaranmak

What are Bug Bounties?

- Many organisations offer cash rewards to researchers for responsibly disclosing security issues or vulnerabilities.
- There are well defined **rules of engagement**, known as “responsible disclosure policies” that outline what is acceptable.
- In other words, **READ THE SCOPE** for each program. They are all different. Don't ruin it for others by blackmailing or feeling entitled to cash.

Advantages of Bug Bounties

For security consultants, students, hobbyists or enthusiasts...

- Perfect to pad out your CV with **real** demonstrable experience.
- It **pays extremely well** when your skill starts increasing.
- There is an excellent global **community** to learn from.
- Learn to distinguish and pursue the **bugs that matter** first.
- They encourage you to think more like a **blackhat** which will make you a better *whitehat*

Advantages of Bug Bounties

For organisations...

- You can still choose who, how and where you want the testing performed.
- You **only** pay for the vulnerabilities found.
- It is more community driven and gives you more of a **community presence**.
- A **larger number of security experts** are looking at your applications.
- Transparency **encourages trust** from your users or clients.
- It's an **additional layer** of security! (Who needs that right?)

Responsible Disclosure Platforms

bugcrowd

- Register as a researcher
- Very researcher focused and encourage skill growth with good feedback.
- Very large variety of programs: web app, mobile & desktop apps, flex (2 week – 1 Month).
- Excellent private bounty programs.
- Almost 20,000 researchers and an active community.
- Encourages finding critical issues with additional rewards.

hackerone

- Register as a researcher
- Larger scoped programs means easier to find bugs.
- Public disclosure of some issues that may help others learn.
- “Internet bug bounty”
- Vendor responses differ greatly
- Higher reward ceiling!

Advice for getting started

- The older programs with smaller applications are likely to have less obvious issues, focus on the newer or larger programs until confident.
- Read the scope, review public bugs for the program.
- Soon after you start building your score or reputation you will start being invited to **private programs**.

Better rewards + less people with access = **more money for you**.

Penetration Testing Methodology

- Information Gathering, Network Reconnaissance & OSINT
- Probing, Active Scanning, Vulnerability Scanning & Analysis
- Exploitation, Leveraging Vulnerabilities & Verification
- Reporting and Communication of issues

Bug Bounty Information Gathering

Regular Techniques:

- Google Searches
- Subdomain Brute Forcing
- AXFR DNS Transfers
- Scanning IP Range
- Reverse DNS lookups
- Web DNS tools
- whois lookups

Recommended Tools:

- dig
- subbrute
- Recon-ng
- gitrob
- Resources:
 - scans.io
 - dnsdumpster.com

Pentest Tips

- Find as many of the organisation owned services or servers as you can.
- The more you find now, the easier it will be to gain access later.
- Reconnaissance and information gathering is by far the **most important step**.
- ALWAYS GO AS DEEP AS YOU CAN.



























































Bug Bounty Information Gathering

“Think Bigger” Attacker Techniques:

- Lookup Company ASN – BGP routers
- Retrieve **ALL** their IP ranges.

Example: Yahoo =>

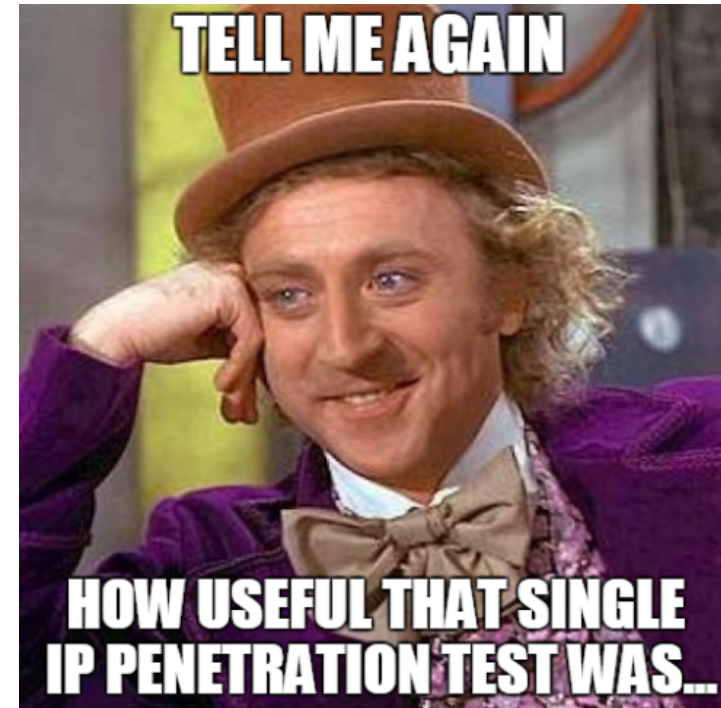
AS7280	Yahoo! Inc.		AS32116	Yahoo!	
AS7233	Yahoo		AS28122	Yahoo! do Brasil Internet Ltda.	
AS58721	Yahoo-Inc		AS26101	Yahoo!	
AS58720	Yahoo-Inc		AS26085	Yahoo!	
AS58525	Yahoo! AUA		AS2521	Yahoo Japan Corporation	
AS5779	Yahoo! Broadcast Services, Inc.		AS24572	Yahoo Japan	
AS55898	Yahoo Japan Corporation		AS24506	YAHOO! TAIWAN	
AS55517	YAHOO! HKA		AS24376	Yahoo China Datacenter	
AS55418	YAHOO! ID1		AS24296	Yahoo Japan Corporation	
AS55417	YAHOO! SGA		AS24236	Yahoo Bangalore Network Monitoring Center	
AS55416	YAHOO! KRA		AS24018	Yahoo Backbone Network, Asia Pacific	
AS4694	Yahoo Japan Corporation		AS23816	Yahoo Japan Corporation	
AS4681	Yahoo Japan Corporation		AS23663	Yahoo Bangalore Network Monitoring Center	
AS45915	Yahoo! India Pvt Ltd.		AS22565	Yahoo	
AS45863	Yahoo! India Pvt Ltd.		AS18140	Yahoo Japan Corporation	
AS45502	Yahoo Corp Network		AS17110	Yahoo	
AS45501	Yahoo Corp Network		AS15896	Yahoo! Europe	
AS43428	Yahoo! Europe		AS15635	Yahoo! Europe	
AS42173	Yahoo! Europe		AS14678	Yahoo	
AS40586	Yahoo! Europe		AS14196	Yahoo	
AS393245	Yahoo		AS131896	Yahoo Japan Corporation	
AS38689	Yahoo! Korea, Corp.		AS10880	Yahoo	
AS38072	Yahoo! Web Services India Pvt Ltd.		AS10310	Yahoo!	
AS38045	Yahoo! Inc. Corp Network		AS10157	Yahoo! Korea, Corp.	
AS36752	Yahoo				
AS36647	Yahoo				
AS36646	Yahoo				
AS36229	Yahoo! Inc.				
AS36129	Yahoo				
AS36088	Yahoo				
AS34082	Yahoo! Europe				
AS34010	Yahoo! Europe				

Bug Bounty Information Gathering

“Think Bigger” Attacker Techniques:

- The couple of hundred target hosts you found before...

Just became a couple of hundred thousand.



Bug Bounty Information Gathering

Other Techniques:

- scans.io data has scans of the whole internet, both http and reverse DNS.
- These JSON dumps are updated weekly.
- Import them into Elasticsearch with Kibana for Information Gathering or searching for your target.

Bug Bounty Vulnerability Scanning

Regular Techniques:

- Scanning Tools
- Custom Scripts

Recommended Tools:

- Nmap, Masscan, Zmap...
- Nessus, OpenVAS...
- Burp, Arachni, Appscan...
- Curl
- Dirb, dirs3arch
- SQLmap
- THC-hydra
- Metasploit

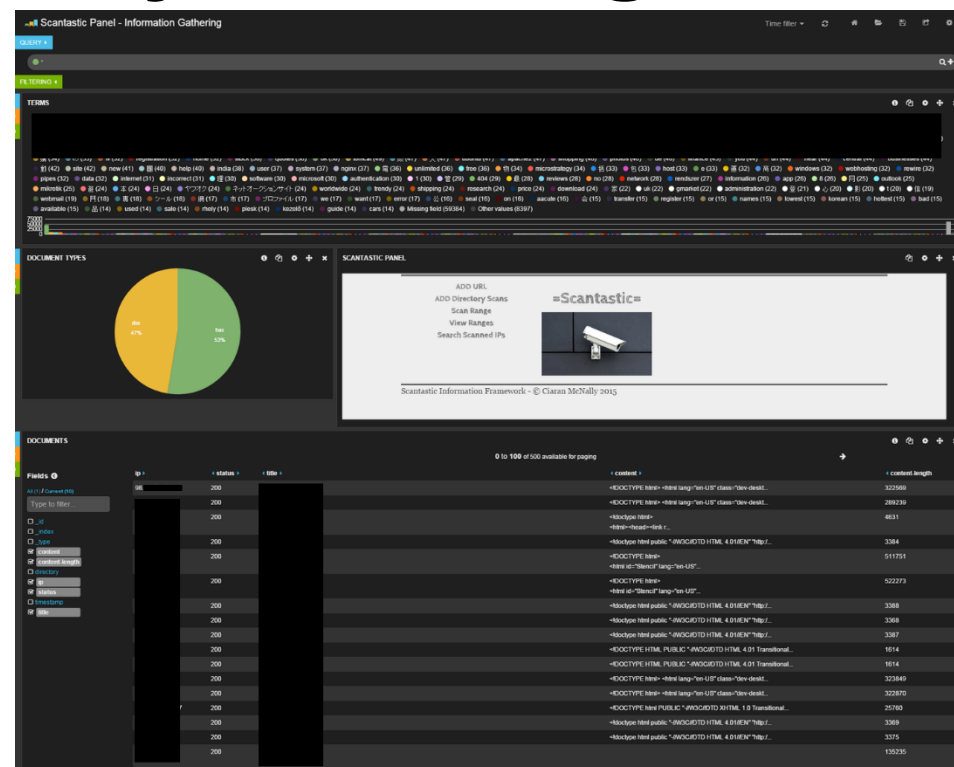
Bug Bounty Vulnerability Scanning

- 99.99% of bounty programs **disallow heavy scanning**. Learn how to effectively throttle your tools if you do opt for mass scanning.
- Organisations running bounties are well capable of running their own scanners. **DO NOT** report “low” or “potential” rated scanner vulnerabilities.

Bug Bounty Vulnerability Scanning

“Think Bigger” Attacker Techniques

- I developed my own threaded scanning tool dubbed “scantastic” in February.
- <https://github.com/maK-/scantastic-tool>
- It dumps masscan network scans and directory brute-forcing scans into elasticsearch.
- Ideas contributed by @nnwakelam



Bug Bounty Vulnerability Scanning

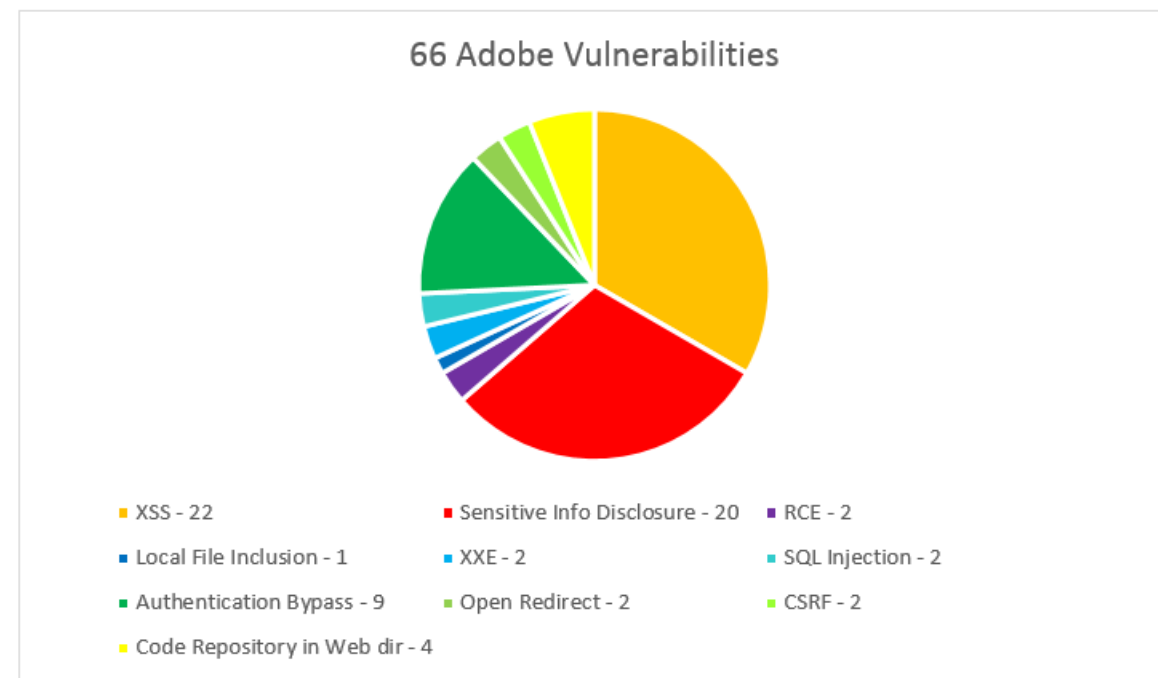
- This is a very powerful technique.
- Once a vulnerability is identified, It can now be scanned for across all services.
- You can also scan for common known vulnerable files and filter the results.

Cluster				Count of alerts	
abuse-content				1208644	
abuse-network				857512	
abuse-other				619915	
bittools				55156	
data-mining				62798	
DataMiningTW				14	
deftools				43584	
devtools				18414	
infraops-other				4866	

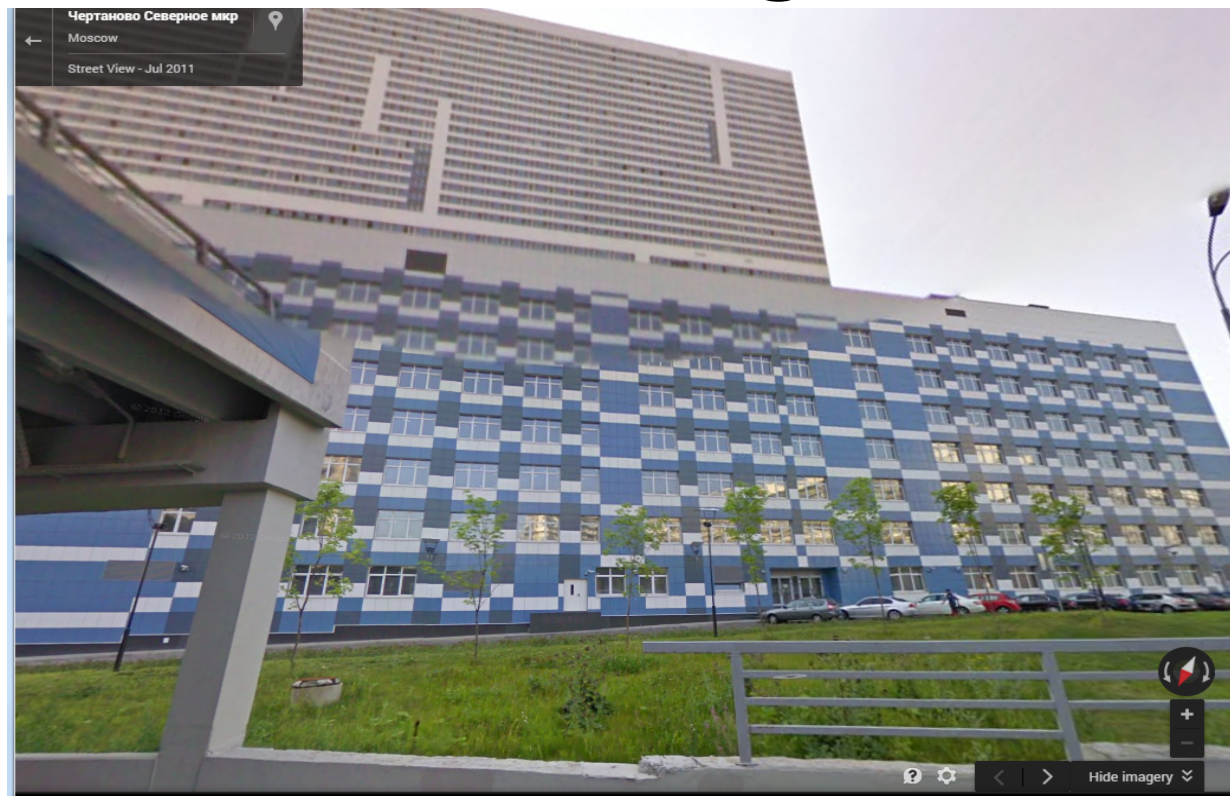
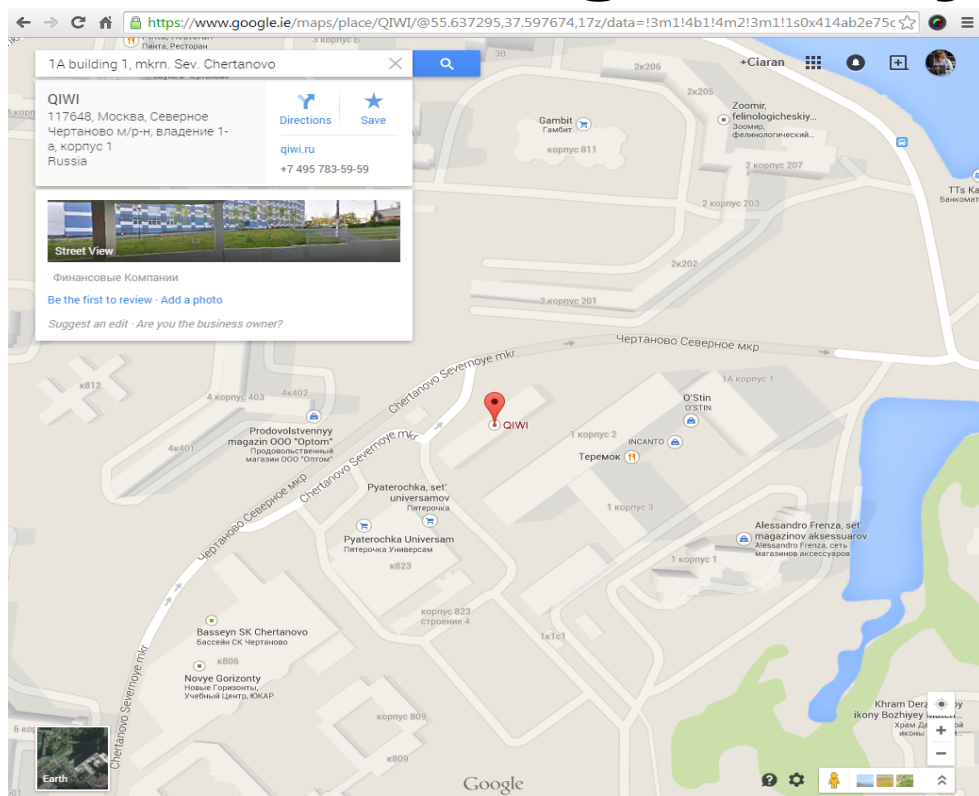
Cluster	Service	Hostname	Timestamp	Status	Message
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-24 04:54:37	UNKNOWN	UNKNOWN between Thu 04:39 - Thu 04:44 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-24 04:49:37	UNKNOWN	UNKNOWN between Thu 04:34 - Thu 04:39 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-24 04:49:37	UNKNOWN	UNKNOWN between Thu 04:34 - Thu 04:39 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-24 04:49:37	UNKNOWN	UNKNOWN between Thu 04:34 - Thu 04:39 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 05:04:37	UNKNOWN	UNKNOWN between Fri 04:49 - Fri 04:54 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 05:04:37	UNKNOWN	UNKNOWN between Fri 04:49 - Fri 04:54 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 05:04:37	UNKNOWN	UNKNOWN between Fri 04:49 - Fri 04:54 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 04:59:37	UNKNOWN	UNKNOWN between Fri 04:44 - Fri 04:49 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 04:59:37	UNKNOWN	UNKNOWN between Fri 04:44 - Fri 04:49 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 04:54:37	UNKNOWN	UNKNOWN between Fri 04:39 - Fri 04:44 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 04:54:37	UNKNOWN	UNKNOWN between Fri 04:39 - Fri 04:44 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 04:54:37	UNKNOWN	UNKNOWN between Fri 04:39 - Fri 04:44 (UTC) thr-monitoring-system-check
test	thr-system-fused_pct	ymsmon-01.ops.corp.sp2.yahoo.com	2014-04-04 04:49:37	UNKNOWN	UNKNOWN between Fri 04:34 - Fri 04:39 (UTC) thr-monitoring-system-check

Bug Bounty Penetration Testing

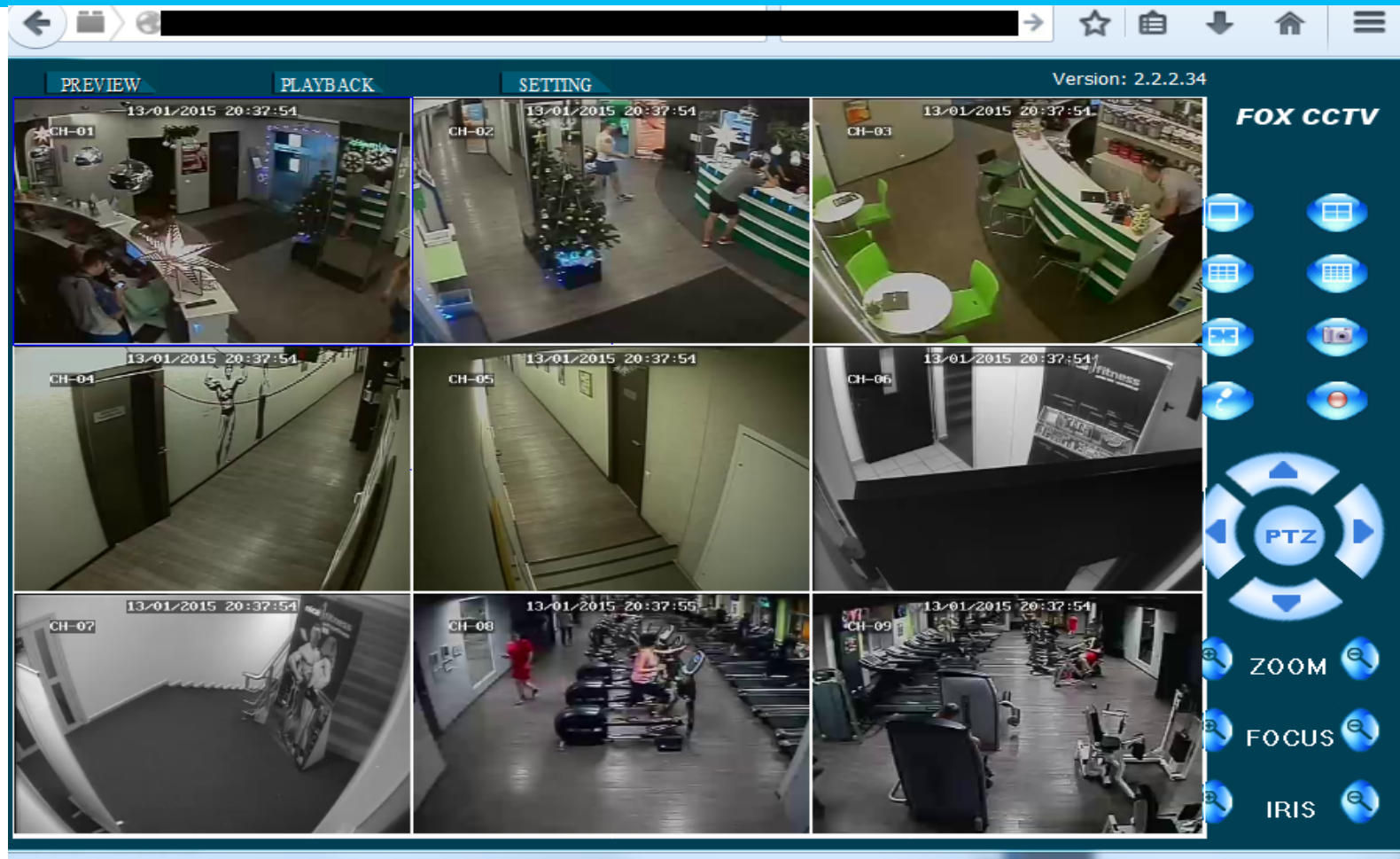
- I combined this scanning technique with a regular penetration testing methodology against Adobe's Responsible Disclosure Program in recent Months.
- Within 24 hours of testing I managed to report 66 Vulnerabilities. I am currently **#1** on the Adobe program as a result.



Bug Bounty Penetration Testing



Password of
"000000"



Bug Bounty Penetration Testing

More Tips:

- You only get rewarded if you are first to find and report an issue. So report first, then update later if you escalate the vulnerability further.
- Expect duplicates
- Always go as far as you can with what you find. The reward could double.
- Keep an eye on **#bugbounty**, **#infosec** or **#bugcrowd** regularly on Twitter, there is a large community always posting there. Plenty of excellent tips and blog posts.

Thank you!

ciaran@securit.ie



Twitter.com/@ciaranmak