💯 FromStart

https://twitter.com/fuxksniper/status/1285211285798322177

Step 1

Domain

(cheak Company Acquistions (means cheak for the root and seed domains) also cheak if the seed domain still own by the main domain owner or not

Using Bluto

darryllane/Bluto

DNS Recon | Brute Forcer | DNS Zone Transfer | DNS Wild Card Checks | DNS Wild Card Brute Forcer | Email Enumeration | Staff Enumeration | Compromised Account Enumeration | MetaData Harvesting Author: Darryl Lane | Twitter: @darryllane101 https://github.com/darryllane/Bluto Give us a vote:

https://github.com/darryllane/Bluto

bluto -d example.com -api 2b0ab19df982a783877a6b59b982fdba4b6c3669 -e

use email Hunter Api

Step 2

Every time you register a domain, you have to provide details about your company or business, such as the name, phone number, mailing address, and specific email addresses for technical and billing purposes. The domain registrar will also store the IP address of your authoritative DNS servers.]\

https://viewdns.com

https://tools.whoisxmlapi.com/reverse-whois-search

use These too to get Whois record and Every thing i mention below

oraganization,inc

asnnumber

domain mail address

nmap

nmap —script dns-brute —script-args dns-brute.domain=$domainnam

(anslookup)

Reverse Whois Reverse Name server

e whois command followed by the target domain name should display some valuable information. The output will contain the registrar name and the Whois server that returned the information. It will also display when the domain was registered and the expiration date

(Amass)

dnsprobe -r cname Mx NS

amass intel -org <company name here>

amass intel -asn <ASN Number Here>

amass intel -cidr <CIDR Range Here>

amass intel -whois -d <Domain Name Here>

Autonomous System Number (ASN) such as: IP owner, registration date, issuing registrar and the max range of the ASN with total IPs. Enter an ASn number, IP address, or a Company name or Email@company.com or domain inc. | (Every website has some registration info on file with the registrars. Companies often own more than one domain so finding these additional assets can help widen your scope.)

Step 3

SUBDOMAIN ENUMARTION

https://twitter.com/pdnuclei/status/1289133795413811201

Once you Done With the Main Domain then Go For Subdomains

> Subdomain Enumaration(subdomains found try to remove the dead once with the help of Resolveing

Resolve the domainlist with filterresolved or masscan or livetargetfinder)

Also use gospider or Gau for finding subdomain

Then Again Run the Subdomain tools on the live One and repeat the resolve step again to resolve

Also Use google dorks for Enumaration

: https://www.exploit-db.com/google-hacking-database/.

inurl:admin site:example.com

"SQL Server Driver][SQL Server]Line 1: Incorrect syntax near"
site:example.com

rapiddns

rapiddns(){
curl -s "

https://rapiddns.io/subdomain/$1?full=1...

" \ | grep -oP '_blank">\K[^<]*' \ | grep -v http \ | sort -u
}

```
Note(if you Found A 404 domain show no access to the data try to run Wayback some Time You can Get some Fruitful things
```

Step 4

Subdomain Brute Force

Subdomain Brute Force is a Tecnique where You Can find The root Domain hidden from normal Access Using

Run a brute force with some custom options:

$ aiodnsbrute -w wordlist.txt -vv -t 1024 domain.com

Altdns

echo -e "######Starting Bruteforce######\n"
altdns -i all.txt -o data_output -w /root/tools/Recon /recon/patterns.txt -r -s results_output.txt

Dnsgen

> is a good one

> cat domains.txt | dnsgen - | massdns -r /path/to/resolvers.txt -t A -o J --flush 2

also use

subrute

#Fastest is Probably SubBrute.py
python $Tools/subbrute/subbrute.py paypal.com paypal.co.uk -t all.txt

subgen

cat SecLists/Discovery/DNS/dns-Jhaddix.txt | subgen -d DOMAIN.TLD | zdns A --name-servers 1.1.1.1 --threads 500 | jq -r "select(.data.answers[0].name) | .name"

Also Go For Virtual Host Discovery

vhostdiscory tool

or

brup

or

Ffuf

Get (rid of) Wildcard Domains

Brute force sub domains (knock,amass,fierce,subfinder,etc)
Run a mutator (dnsgen,syborg,etc)
Resolve the mutations
Feed gwdomains the mutated sub domains
Run
cat mutated.txt | gwdomains

Note

- [ ] Then Resolve These Output subdomain with

```
liveTargetFinder
```

Step 5

Fingerprint

Cms

https://whatcms.org/

Identify the Cms then use the Scanner)FOR Wordpress Site use `WPScan` |for `drupal joomla scanner`

https://git clone https://github.com/Dionach/CMSmap.git

rezasp/joomscan
OWASP Joomla! Vulnerability Scanner (JoomScan) is an open source project, developed with the aim of automating the task of vulnerability detection and reliability assurance in Joomla CMS deployments. Implemented in Perl, this tool enables seamless and effortless scanning of Joomla installations, while
https://github.com/rezasp/joomscan

thomashartm/burp-aem-scanner
Burp AEM Security Scanner is an AEM focussed plugin which supports the evaluation of well known misconfigurations of AEM installations. It supports the verification of a number of Adobe's security checklist topics and evaluates typical AEM and Dispatcher misconfigurations. AEM is an enterprise
https://github.com/thomashartm/burp-aem-scanner

Use Nikto for every fingerprinting subdomain You Have in Your Found List

Nikto |

nikto -h <ip>or<domainname> -ssl (ssl enable website)

WafW00f<it Detect Which Firewall is the Website using >

```
wafw00f <domainname>
Youcan Also Use Nmap for Detecting WAF
 nmap -p 80,443 --script=http-waf-detect <domainname>
```

web application firewalls

| whatweb

command

```
whatweb <domainname>
```

Builthwith

Chrome Extention

https://builtwith.com/

Identify The Tecnology Of the Website

Wapplayzer

Chrome Extention it Also Identify The Tecnology

Once You Identify the tecnolgy Serach For the C

Cname

Identify The Cname of Every subdomain for the takeover (also look for nameserver domain | and Mailserver domain) takeover

```
if a site uses
1 AngularJS,
 test {{7*7}} to see whether 49 is rendered anywhere.
If the application is built with ASP.NET with XSS protection
enabled, you might want to focus on testing other vulnerability
types first and check for XSS as a last resort.
If a site is built with
2 Rails,
 you might know that URLs
typically follow a /CONTENT_TYPE/RECORD_ID pattern, where the
RECORD_ID is an autoincremented integer. Using HackerOne as
an example, report URLs follow the pattern
www.hackerone.com/reports/12345. Rails applications
commonly use integer IDs, so you might prioritize testing
insecure direct object reference vulnerabilities because this
vulnerability type is easy for developers to overlook.
If an API returns
3 :JSON or XML
, you might recognize that
those API calls unintentionally return sensitive information
that isn't rendered on the page. Those calls might be a good
testing surface and could lead to information disclosure
vulnerabilities.
Here are some factors to keep in mind at this stage:
Content formats a site expects or accepts For example,
XML files come in different shapes and sizes, and XML
parsing can always be associated with XXE vulnerabilities.
Keep an eye out for sites that accept .docx, .xlsx, .pptx, or
other XML file types.
Third-party tools or services that are easily
misconfigured Whenever you read reports about hackers
exploiting such services, try to understand how those
reporters discovered the vulnerability and apply that
process to your testing.
Encoded parameters and how an application handles
them Oddities might be indicative of multiple services
interacting in the backend, which could be abused.
Custom implemented authentication mechanisms, such
```

```
as OAuth flows Subtle differences in how an application
handles redirect URLs, encoding, and state parameters
might lead to significant vulnerabilities.
```

`Step 6`

Crawling

Tip: Never forget to look for hidden parameters in the source code. click view source code and search for “hidden”, “input”, or “var” parameters.

(Basic Crawling Crawling a website is typically one of the first places to start once you have discovered the live endpoints. It basically involves recursively visiting and saving each link on a website)

> ***Scan The List of Live URL you found Above in step 3 $ 4***

During Crawling You Will Found Alots of Endponts use Gf Tomnomnom and search for differnt parameters

1ndianl33t/Bug-Bounty-Roadmaps

The Bug Hunter's Methodology v4 Roadmap SSRF Techniques Roadmap Web Penetration Tester Roadmap Mobile Penetration Tester Roadmap Server_Side_Template injection Roadmap More Roadmaps You can encourage me to contribute more to the open source with donations. 8085778875

https://t.co/ODoSQlRrBd?amp=1

(Linked And Js Discovery "End Points | Looking For JS File And search For keys password and config Files"
Grep Endpoint from Js File cheak the status of the JavaScript files using hakcheckurl |use JS Beautifier for reading the js file)

Gospider

```
gospider -s "https://google.com/" -o output -c 10 -d 1
gospider -S sites.txt -o output -c 10 -d 1
```

Gau

```
gau example.com
```

KathanP19/JSFScan.sh

Contribute to KathanP19/JSFScan.sh development by creating an account on GitHub.

https://github.com/KathanP19/JSFScan.sh

- [ ] There is another Tool I Will Add it Later

Step 7

Screen Shots

Eyewitness

```
./EyeWitness -f urls.txt --web

./EyeWitness -x urls.xml --timeout 8

./EyeWitness.py -f urls.txt --web --proxy-ip 127.0.0.1 --proxy-port 8080 --proxy-type socks5 --timeout 120
```

Aquatone

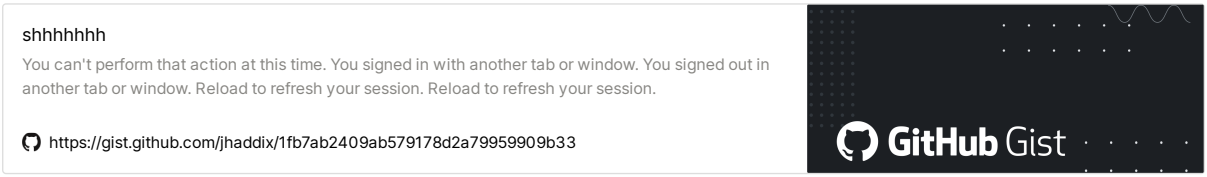
$$cathosts.txt|aquatone - out\ /aquatone/example.com$$

Step 8

Github Recon

Tools

Use



SecreatSearch.py Tool

Also use

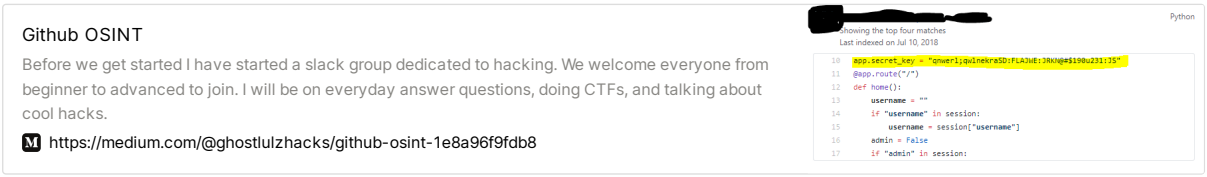
Subdominzer

To Get some Secerts

Secreat Finder

go get github.com/michenriksen/gitrob

Manual




```
filename:sftp-config.json password.
filename:.env MAIL_HOST=smtp.gmail.com
filename:.npmrc _auth
filename:.dockercfg auth
extension:pem private
extension:ppk private
filename:id_rsa or filename:id_dsa
extension:sql mysql dump
extension:sql mysql dump password
filename:credentials aws_access_key_id
filename:.s3cfg
filename:wp-config.php
filename:.htpasswd
filename:.env DB_USERNAME NOT homestead
filename:.env MAIL_HOST=smtp.gmail.com
filename:.git-credentials
*"target(.)com" password
*"target(.)com" "pass" 'email'
*"target(.)com" "api"
*"target(.)com" FTP
*"target(.)com" SMTP
*"target(.)com" LDAP
*"target(.)com" PEM (For Keys)
"http://hackerb0y.com" "password"
"http://hackerb0y.com" "database"
"http://hackerb0y.com" "secret"
"http://hackerb0y.com" "api_key"
```

"site . com" ssh language:yaml
Got config.yaml

Dork:
"Url" filename:automation password passwd pass

intitle:"index of" "ssh.yml"
intitle:"index of" "database-old.yml"
intitle:"index of" "configuration.yml"
intitle:"index of" "database.yml"
intitle:"index of" "ftp.yml"

Another Dork
"target . com" sshpass
Remove space :)
Note: Target must have oarge scope. Good chances to get juicy information
Best URL:

https://google.com/search?q=how+to:+your%20question+here...

pip install truffleHog

If You foound Any Git file return 404 try this tool

lijiejie/GitHack

GitHack is a .git folder disclosure exploit. It rebuild source code from .git folder while keep directory structure unchanged. GitHack是一个.git泄露利用脚本，通过泄露的.git文件夹下的文件，重建还原工程源代码。 渗透测试人员、攻击者，可以进一步审计代码，挖掘：文件上传，SQL注射等web安全漏洞。 解

https://t.co/FzXHh15Fco?amp=1

Google Dorks

site:http://ideone.com | site:http://codebeautify.org | site:http://codeshare.io | site:http://codepen.io | site:http://repl.it | site:http://justpaste.it | site:http://pastebin.com | site:http://jsfiddle.net | site:http://trello.com "alibaba.com

Google Dork for API hacking You can always find updated dork list from https://github.com/mrnitesh/WSDL/blob/master/dork.txt

Trello	site:trello.com "Company Name"	Trello is a web based Kanban board. This is often used to find credentials and internal links of organizations.
Prezi	site:prezi.com "Company Name"	This site is used to make presentations and can sometimes contain internal links and credentials.
Jsdeliver	site:jsdelivr.net "Company Name"	CDN for NPM and GitHub.
Codepen	site:codepen.io "Company Name"	Codepen is an online tool for creating/testing front end code. You can sometimes find API keys and other credentials in here
Pastebin	site:pastebin.com "Company Name"	Pastebin is a site where people upload text documents typically for sharing. You can often find internal documents and credentials in here. Hackers also use this site to share database leaks.
Repl	site:repl.it "Company Name"	Repl is an online compiler. You can sometimes find hard coded credentials in users scripts. I have personally used this to compromise a few targets.
Gitter	site:gitter.im "Company Name"	Gitter is an open source messaging platform. You can sometimes find private messages containing credentials, internal links, and other info.

Name	Dork	Description
Codepad	site:codepad.co "Company Name"	Codepad is an online compiler/interpreter. You can sometimes find hard coded credentials here.
Scribd	site:scribd.com "Company Name"	Scribd is known for their books and E-books but you can sometimes find internal files uploaded by employees that contain passwords
NPM	site:npmjs.com "Company Name"	Use this to find NodeJS source code used by a company
NPM	site:npm.runkit.com "Company Name"	Use this to find NodeJS source code used by a company

Libraries IO	site:libraries.io "Company Name"	Libraries.io is a web service that lists software development project dependencies and alerts developers to new versions of the software libraries they are using.
Coggle	site:coggle.it "Company Name"	Coggle is used to create mind maps. You might be able to find internal flow charts which contain credentials
Papaly	site:papaly.com "Company Name"	This site is used to save bookmarks and links. You can sometimes find internal links, documents, and credentials.

Name	Dork	Description
Codepad	site:codepad.co "Company Name"	Codepad is an online compiler/interpreter. You can sometimes find hard coded credentials here.
Scribd	site:scribd.com "Company Name"	Scribd is known for their books and E-books but you can sometimes find internal files uploaded by employees that contain passwords
NPM	site:npmjs.com "Company Name"	Use this to find NodeJS source code used by a company
NPM	site:npm.runkit.com "Company Name"	Use this to find NodeJS source code used by a company

Ghostsulz AKA Alex Thomas
Page | 113

Libraries IO	site:libraries.io "Company Name"	Libraries.io is a web service that lists software development project dependencies and alerts developers to new versions of the software libraries they are using.
Coggle	site:coggle.it "Company Name"	Coggle is used to create mind maps. You might be able to find internal flow charts which contain credentials
Papaly	site:papaly.com "Company Name"	This site is used to save bookmarks and links. You can sometimes find internal links, documents, and credentials.

Shodan

Use Shodan..py For Searching Vulnerbilty in shodan

KathanP19/portscan.sh

All in one port scanning script. Contribute to KathanP19/portscan.sh development by creating an account on GitHub.

https://github.com/KathanP19/portscan.sh/blob/master/portscan.sh

Step 9

Go For Subdomain Takeover

Get A List of Subdomain YOu Found In the Step 3 and Run some Subdomain takeover tools Againts the list of subdomains

Also Go For NameServer Domain | Mail Server domain

mandatoryprogrammer/TrustTrees

TrustTrees is a script to recursively follow all the possible delegation paths for a target domain and graph the relationships between various nameservers along the way. TrustTrees also allows you to view where errors occurred in this chain such as DNS REFUSED, NXDOMAIN, and other errors.

https://github.com/mandatoryprogrammer/TrustTrees

https://digi.ninja/files/bucket_finder_1.1.tar.bz2

echo "[+] S3 Bucket Scanner [+]"

echo "[+] TKO-SUBS for Subdomain TKO [+]"

echo "[+] SUBJACK for Subdomain TKO [+]"

Nuclei

Subover

Step 10

NEW CVE(use Nuclei)

If There you See Any new Remote 0day Cve Try

Nuclei

Jaeles

Step 11

Crawling

(Basic Crawling Crawling a website is typically one of the first places to start once you have discovered the live endpoints. It basically involves recursively visiting and saving each link on a website)

use This Scannre and cheak for owasp vulnerbilties

pikpikcu/XRCross

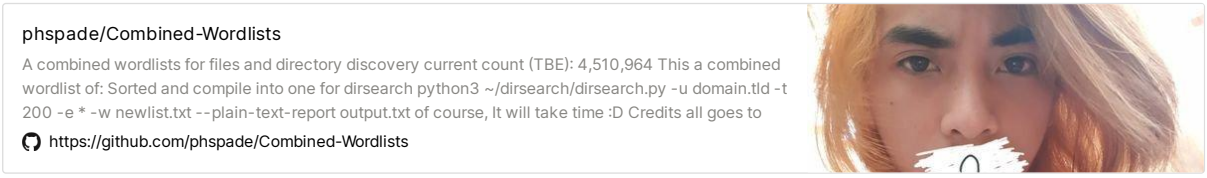
Details XRCross is a Reconstruction, Scanner, and a tool for penetration / BugBounty testing.

https://github.com/pikpikcu/xrcross

Step 12

Directory Brute Force

Try to Use A Good Word List or Use | Raftsmall |jhadix all.txt | RobotsDisallowed1000.txt



Directory Brute Forceing using

dirsearch

python3 dirsearch.py -e conf,config,bak,backup,swp,old,db,sql,asp,aspx,aspx~,asp~,py,py~,rb,rb~,php,php~,bak,bkp,cache,cgi,conf,csv,html,in -u https://coderedmarketing.eccouncil.org/ -t 100 -w /root/tools/bruteforce/ffufplus/wordlist/dicc.txt -b

https://twitter.com/faizalabroni/status/1283939826203365378

Ffuf

Use Ffuf plus For directory Brute Force With Defult Word List

`(also brute force login page maintarget and there others page too )`

STEP 12

ParaMeter Discovery

Arjun

```
python3 arjun.py -u https://api.example.com/endpoint --get
```

s0md3v/Arjun

To find GET parameters, you can simply do: python3 arjun.py -u https://api.example.com/endpoint --get Similarly, use --post for POST and --json to look for JSON parameters. A list of URLs stored in a file can be test by using the --urls option as follows python3 arjun.py --urls targets.txt --get Arjun uses 2

https://github.com/s0md3v/Arjun/wiki/Usage#scanning-a-single-url

Ffuf

Use Ffuf Plus For Parameter Finding

dark-warlord14/ffufplus

You can read the writeup on this script here Dismiss GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together. Sign up Permalink Failed to load latest commit information. ffufplus - ffuf on Steroids bash install.sh To run the

https://github.com/dark-warlord14/ffufplus

PARAMSPIDER

devanshbatham/ParamSpider

Finds parameters from web archives of the entered domain. Finds parameters from subdomains as well. Gives support to exclude urls with specific extensions. Saves the output result in a nice and clean manner.

https://github.com/devanshbatham/ParamSpider

```
python3 paramspider.py --domain bugcrowd.com --exclude woff,css,js,png,svg,php,jpg --output bugcrowd.txt
```

> we Have Also Collected some end points During the Perivous Step also combine Both of them and go for the hunt

`For Finding Hidden parameter And endpoints`

STEP 14

Port Scan

vesche/scanless

online port scan scraper. Contribute to vesche/scanless development by creating an account on GitHub.

https://github.com/vesche/scanless

sudo nmap -sS -T4 -sC -oA myreportname — stylesheet https://raw.githubusercontent.com/honze-net/nmap-bootstrap-xsl/master/nmap-bootstrap.xsl -iL subdomain.txt

nmap –script smtp-enum-users.nse
nmap -vv -p0- -sSUV -O -oA

Nmap -sV -sC -v -T4 --script http-shellshock -p 443,80 <target>

nmap -vv -p0- -sSUV -O -oA $outputfile $targe

nmap -sV --script "discovery, vuln, not (brute or dos)" --script-timeout 30m --host-timeout 35m -T4 <TARGETGOESHERE> -oA <OUTPUTFILENAMEHERE>

Using Nmap or Massscan And

KathanP19/portscan.sh
All in one port scanning script. Contribute to KathanP19/portscan.sh development by creating an account on GitHub.
https://github.com/KathanP19/portscan.sh

Pass The Result To Brutespray for bruteforceing SSH services,FTP SMTP AND some Others

Brutespray

x90skysn3k/brutespray
Created by: Shane Young/@x90skysn3k && Jacob Robles/@shellfail Inspired by: Leon Johnson/@sho-luv Credit to Medusa: JoMo-Kun / Foofus Networks - http://www.foofus.net https://youtu.be/C-CVLbSEe_g BruteSpray takes nmap GNMAP/XML output or newline seperated JSONS and
https://github.com/x90skysn3k/brutespray

```
python brutespray.py --file nmap.gnmap
```

TOP 10 OWASP VULNERBILTIES

Use This To Find Some Cool Stuff

ethicalhackingplayground/Zin
A Payload Injector for bugbounties written in go. Contribute to ethicalhackingplayground/Zin development by creating an account on GitHub.
https://github.com/ethicalhackingplayground/Zin

Google Dorks (also use for ssrf xss information disclosure and buckets misconfigration)

Spf Record

Chainlink disclosed on HackerOne: No Valid SPF Records.

Hiii, There is any issue No valid SPF Records Desciprition : There is a email spoofing vulnerability.Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

https://hackerone.com/reports/629087

Cors Misconfigration (gf cors,corsme scanner)

One Liners For Cors

```
cors_reflect_auto(){
        gau $1 | while read url;do target=$(curl -s -I -H "Origin: https://evil.com" -X GET $url) | if grep 'https://evil.com';
}
cors_null_origin(){
        gau $1 | while read url;do target=$(curl -s -I -H "Origin: null" -X GET $url) | if grep 'Access-Control-Allow-Origin: n

}
cors_null_value(){
        gau $1 | while read url;do target=$(curl -s -I -X GET "$url") | if grep 'Access-Control-Allow-Origin: null'; then echo
}
cors_trust_subdomain(){
        gau $1 | while read url;do target=$(curl -s -I -H "Origin: evil.$url" -X GET "$url") | if grep 'Access-Control-Allow-Or
}
cors_domain_not_valid(){
        gau $1 | while read url;do target=$(curl -s -I -H "Origin: https://not$site" -X GET "$url") | if grep 'Access-Control-A
}
cors_dom_ext(){
        gau $1 | while read url;do target=$(curl -s -I -H "Origin: $site.evil.com" -X GET "$url") | if grep "Origin: Access-Con
}
```

Shivangx01b/CorsMe

A cors misconfiguration scanner tool based on golang with speed and precision in mind ! Reflect Origin checks Prefix Match Suffix Match Not Esacped Dots Null ThirdParties (Like ⇒ github.io, repl.it etc.) SpecialChars (Like ⇒ "}","(", etc.) $ go get -u github.com/shivangx01b/CorsMe Single Url echo

https://github.com/Shivangx01b/CorsMe

Email Header Injection on Reset Password Function

Mavenlink disclosed on HackerOne: Password reset link injection...

@cablej found a vulnerability in our password reset functionality that allowed an attacker using an HTTP request with a modified `Host` header to cause a password reset link to be emailed to the target user that would navigate to the attacker's domain.

https://hackerone.com/reports/281575

SMTP Injection And Host Header Injection

LocalTapiola disclosed on HackerOne: SMTP configuration...

Issue The reporter found a few misconfigurations in one smtp-server related to the viestinta.lahitapiola.fi domain. ##Fix Some configuration changes were made to the smtp-service. ##Reasoning The issues reported were investigated thoroughly. The service has underlying controls which make misuses in the

https://hackerone.com/reports/183548

New Relic disclosed on HackerOne: Host Header Injection

Reproduction 1- open reset link https://login.newrelic.com/passwords/forgot 2- Enter the victim's email address and click Reset and Email Password 3- Intercept the HTTP request in Burp Suite & add X-Forwarded Host Header and write attacker.com/.newrelic.com link will be like...

https://hackerone.com/reports/698416

Boozt Fashion AB disclosed on HackerOne: Email link poisoning /...

Description ---------- It is possible to poison the link of the password reset email. This is generally done by altering the [Host header](http://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html), but in this case, the WAF is successfully blocking it. The trick here is to add an **X-

https://hackerone.com/reports/182670

IFrame ClickJacking

Gratipay disclosed on HackerOne: Bypassing X-frame options

bypass X-Frame-Options (Proxy protection NOT used) DomainUsing: gratipay.com Proxy protection NOT used , i can bypass X-Frame-Options header and recreate clickjacking on the whole domain. I see that you don't have a reverse proxy protection this allows all users to proxy your website rather than

https://hackerone.com/reports/283951

OLX disclosed on HackerOne: Bypass CSP frame-ancestors at...

Hi, [olx.co.za](https://www.olx.co.za/) and [olx.com.gh](https://www.olx.com.gh/) both of them restrict framing by using this CSP rule: ``` content-security-policy: frame-ancestors 'self' https://*.mod-tools.com:* ``` olx.co.za: {F313178} olx.com.gh: {F313179} If we take a look at `mod-tools.com` we can

https://hackerone.com/reports/371980

Improper Access Control

Vend VDP disclosed on HackerOne: Improper access control on adding...

Summary:** User without permissions to add a Register to an Outlet can bypass this restriction and add a Register to an Outlet. **Description:** I do not know which permission exactly controls this action, I tested this against default `Cashier` role. User with default `Cashier` role has no permission to add

https://hackerone.com/reports/317332

GitLab disclosed on HackerOne: Attacker is able to access commit...

Summary:** [add summary of the vulnerability] **Description:** [add more details about this vulnerability] ## Steps To Reproduce: To reproduce this vulnerability, we need two accounts, lets say those accounts are: -> victim@gmail.com -> attacker@gmail.com - Create a project from account

https://hackerone.com/reports/502593

Parameter Tempering

WordPress disclosed on HackerOne: Parameter tampering : Price...

Hello Security Team, I have found that you can buy any products in less amount or even we can say as free by changing the price of the product!! POC : 1) go to https://mercantile.wordpress.org/ 2) choose any product and add to cart 3) Now go to cart add your billing details 4) Intercept request with burpsuite and

https://hackerone.com/reports/682344

Shipt disclosed on HackerOne: Price manipulation via fraction...

A security researcher identified an issue in our member application that showed how a user's cart would accept fractional quantities of any item; irrespective of whether or not the item was capable of being in a 'fractional' state (e.g. fractional quantities were being accepted for a half pound of ground beef, but were

https://hackerone.com/reports/388564

HTTP PARAMETER POLLUTION

HackerOne disclosed on HackerOne: HTTP Parameter Pollution using...

Using semicolons, I was able to override the `for` parameter in the iframe element. This allowed me to load external Greenhouse forms (which are not owned by HackerOne) on the page. Later on, a global fix was applied by Greenhouse on the `boards.greenhouse.io/embed/` endpoint.

https://hackerone.com/reports/298265

Slack disclosed on HackerOne: HTTP parameter pollution from...

Slack's career page was using an outdated Greenhouse JavaScript dependency which resulted in an HTTP parameter pollution vulnerability. This would have allowed the loading of external Greenhouse forms (not owned by Slack). We updated the Javascript and the issue is resolved. Thanks @irvinlim!

https://hackerone.com/reports/335339

TEMPLATE INJECTION

Shopify disclosed on HackerOne: H1514 Server Side Template...

Full story with explanation of how this was exploited can be found here: https://mahmoudsec.blogspot.com/2019/04/handlebars-template-injection-and-rce.html

https://hackerone.com/reports/423541

Unikrn disclosed on HackerOne: Urgent: Server side template...

Hi All, I've found an issue which has allowed me to execute file_get_contents and extract your /etc/passwd file. ##Description It appears as though you are using smarty on the backend for templating. Entering a malicious payload as my firstname, lastname and nickname and then inviting a user to join the

https://hackerone.com/reports/164224

Rockstar Games disclosed on HackerOne: Client-side Template...

In this report, the researcher was able to perform [AngularJS Template Injection] (https://hackerone.com/redirect?signature=49c7114e65f27ab7700511ac15aaa633cf22a68b&url=http%3A%2F%2Fblog.portswigger.net%

https://hackerone.com/reports/271960

OAUTH VULNERABILITIES

TTS Bug Bounty disclosed on HackerOne: Stealing Users OAuth Tokens...

I found that https://login.fr.cloud.gov/oauth/authorize has vulnerability by open redirect on oauth redirect_uri which can lead to users oauth tokens being leaked to any malicious user. Step : 1, Clicked on link https://login.fr.cloud.gov/oauth/authorize?

https://hackerone.com/reports/665651

BOHEMIA INTERACTIVE a.s. disclosed on HackerOne: Stealing Users...

Hi, I would like to report an Open redirection on oauth redirect_uri which can lead to users oauth tokens being leaked to any malicious user. **Detail** During the OAUTH flow, the redirect_uri on https://accounts.bistudio.com is not properly validating that the URL given is proper, as such a bypass of

https://hackerone.com/reports/405100

Broken Link Cheak

GitLab disclosed on HackerOne: Impersonation attack via Broken Link...

Summary A link on `https://about.gitlab.com/resellers/` was broken and could've allowed a user to impersonate a reseller and attack / scam your customers. ## Proof of Concept 1.) Visit https://about.gitlab.com/resellers/ 2.) Hit `Ctrl+F` and find "intenso" {F219301} 3.) Now click the

https://hackerone.com/reports/266908

Legal Robot disclosed on HackerOne: Broken links for stale domains...

Hi, URL: https://www.legalrobot.com/press/2016/07/07/tech4good-on-a-global-scale/ Broken link for an expired domain which is available for sale: http://ecotechfoundation.net/ You may verify that it is available for sale @ https://www.secureserver.net/domains/searchresults.aspx?

https://hackerone.com/reports/276244

Gratipay disclosed on HackerOne: Broken link for stale DNS entry...

Hi Team, Page: https://gratipay.com/Breadcrumbel/ Broken link for stale DNS entry: ``` Homepage ``` Root domain breadcumbry.com has expiration date: Registrar Registration Expiration Date: 2018-06-10T18:18:30Z And also from whois: Domain Status: OK https://icann.org/epp#ok OK status means it has

https://hackerone.com/reports/279351

Gratipay disclosed on HackerOne: Broken link for stale DNS entry...

Hi Team, Page: https://gratipay.com/Breadcrumbel/ Broken link for stale DNS entry: ``` Homepage ``` Root domain breadcumbry.com has expiration date: Registrar Registration Expiration Date: 2018-06-10T18:18:30Z And also from whois: Domain Status: OK https://icann.org/epp#ok OK status means it has

https://hackerone.com/reports/279351

CSRF Login And Logout\

Tool

xsrfprobe --help

WakaTime disclosed on HackerOne: Logout CSRF

Cross-Site Request Forgery (CSRF) logout application Because of that gap, he updates a man's attack in the middle and is exposed to the agent and all his personal data at risk This may cause the web to be compromised I will send a test script and a video explaining everything about the problem Resource

https://hackerone.com/reports/244778

HackerOne disclosed on HackerOne: (HackerOne SSO-SAML) Login CSRF,...

Summary:### Login CSRF, Open Redirect, and Self-XSS Possible Exploitation through HackerOne SSO-SAML ###PoC### - Go to [redacted]; Use a browser window with clear cookies. Source-code: ``` setTimeout(function(){document.location.href =...

https://hackerone.com/reports/171398

SQL Header based And Cookie Based

Instacart disclosed on HackerOne: Cookie-Based Injection

Hi** Security Team instacart I'm Found Vulnerability **Cookie-Based Injection** It's may be possible to steal or manipulate session and cookies if attacker can injection **XSS** . details --- in path **/help/** contain header in cookie paramter **ahoy_visitor** and **ahoy_visit** it's allow injection because re

https://hackerone.com/reports/105419

Zomato disclosed on HackerOne: [https://reviews.zomato.com] Time...

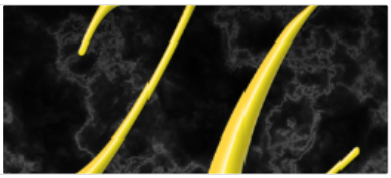
@samengmg found an cookie based SQL injection on https://reviews.zomato.com.

https://hackerone.com/reports/300176

Paragon Initiative Enterprises disclosed on HackerOne: Blind SQL INJ

The test result seems to indicate a vulnerability because the response contains SQL Server errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters. The following changes were applied to the original request: Added HTTP header

https://hackerone.com/reports/115304



SSRf (Finding SSRF Parameter Using Hunt Brup Pulgin or gf ,json (against The crawl Data U Found at The Crawling step)

Node.js third-party modules disclosed on HackerOne: Server-Side...

I would like to report about SSRF vulnerability in CMS Ghost blog It allows attacker able to send a crafted GET request from a vulnerable web application # Module **module name:** ghost **version:** 3.5.2 **npm page:** `https://www.npmjs.com/package/ghost` **website page** `https://ghost.org/` ##

https://hackerone.com/reports/793704

TTS Bug Bounty disclosed on HackerOne: SSRF in Search.gov via ?url=...

Summary: `https://search.usa.gov/help_docs` endpoint is vulnerable to SSRF via `url` parameter. The parameter is protected but can be bypassed using LF (%0A). # Steps To Reproduce: 1. Login to Search.gov and click `help manual`. 2. The following request was vulnerable. - Request ``` GET

https://hackerone.com/reports/514224

Xss

Easy Automation XSS Tip

cat subdomains.txt | waybackurls >> wayback.txt

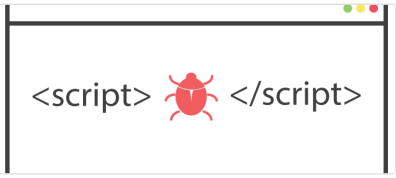
cat subdomains.txt | hakrawler -depth 3 -plain >> spider.txt

cat spider.txt wayback.txt | kxss == XSS $$$

Top 25 XSS Bug Bounty Reports

In this article, we will discuss Cross-Site Scripting (XSS) vulnerability, how to find one and present 25 disclosed reports based on this issue. XSS stands for Cross-Site Scripting and it is a web-based vulnerability in which an attacker can inject malicious scripts (usually JavaScript) in the application.

https://medium.com/@corneacristian/top-25-xss-bug-bounty-reports-b3c90e2288c8



Twitter disclosed on HackerOne: Stored XSS on reports.

Summary:** Stored XSS can be submitted on reports, and anyone who will check the report the XSS will trigger. **Description:** Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.

https://hackerone.com/reports/485748

HackerOne disclosed on HackerOne: Reflected XSS on...

Good day :) I hope your doing as well as can be during these difficult times. I have found xss at 2 endpoints: https://www.hackerone.com/resources/ and https://resources.hackerone.com The payloads that work are...

https://hackerone.com/reports/840759

(Using Hunt Brup Pulgin or Shive gf json (against The crawl Data U Found at The Crawling step) File or Some One liners

Cheak Cryptograpy in Reset Function

Revive Adserver disclosed on HackerOne: Authentication Bypass by...

Hi, This is a fun bug I came across while doing a pentest for a client, after going through Revive Advserver's code for a few hours, I found this authentication bypass. This vulnerability seem to affect all versions, including the latest one, I was sent by one of your developers to report it here.

https://hackerone.com/reports/576504

Uber disclosed on HackerOne: Issue with Password reset functionality

Dear Team, There are password change issues with uber. there are two issues: 1)User is not receiving notification when he reset password via password reset link. 2)Password reset link is not expiring after used once. Good thing: when user change his info like profile update, password change.

https://hackerone.com/reports/92251

Unicode injection in Email Parameter @

Unikrn disclosed on HackerOne: HTML injection in email in unikrn.com

NOTE! Thanks for submitting a report! Please replace *all* the [square] sections below with the pertinent details. Remember, the more detail you provide, the easier it is for us to verify and then potentially issue a bounty, so be sure to take your time filling out the report!

https://hackerone.com/reports/262004

HackerOne disclosed on HackerOne: mailto: link injection on...

I just found that entering a non-existing porogram returns the following response: >The Directory doesn't have a profile matching these criteria. >If an organization has published security contact information or a vulnerability disclosure policy, **please let us know.** The bold part has a mailto: link which is in

https://hackerone.com/reports/66262

Bypassing Rate Limit

Headers:- X-originating-IP:ip
| X-Forwarded-FOR:ip
| X-Remote-IP:ip
| X-Remote-Addr
| X-Client-IP:ip
| X-Forwarded-Host:ip)

Slack disclosed on HackerOne: Rate-limit bypass

Hello Slack, This vulnerability is about a 2FA Bypass, On Slack Web Application there is rate limit implemented. After performing 4-6 failed 2FA Attempt, Rate limit logic will ge Triaged and ask user to wait for next attempt(preventing automated 2FA Attempts) I tested the same using iOS App(iOS 9.3.3

https://hackerone.com/reports/165727

HackerOne disclosed on HackerOne: Bypass rate limiting on...

A blog post was released after discovering this issue here: https://zseano.com/tut/3.html

https://hackerone.com/reports/170310

Request Smuggling

Brave Software disclosed on HackerOne: HTTP Request Smuggling

When malformed or abnormal HTTP requests are interpreted by one or more entities in the data flow between the user and the web server, such as a proxy or firewall, they can be interpreted inconsistently, allowing the attacker to "smuggle" a request to one device without the other device being aware of it.

https://hackerone.com/reports/866382

Slack disclosed on HackerOne: Mass account takeovers using HTTP...

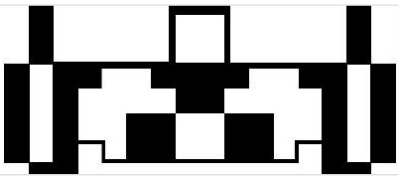
This researcher exploited an HTTP Request Smuggling bug on a Slack asset to perform a CL.TE-based hijack onto neighboring customer requests. This hijack forced the victim into an open-redirect that forwarded the victim onto the researcher's collaborator client with slack domain cookies. The posted

https://hackerone.com/reports/737140

defparam/smuggler

An HTTP Request Smuggling / Desync testing tool written in Python 3 A special thanks to James Kettle for his research and methods into HTTP desyncs And a special thanks to Ben Sadeghipour for beta testing Smuggler and for allowing me to discuss my work at Nahamcon 2020 This tool does not

https://github.com/defparam/smuggler



RCE

Top 25 RCE Bug Bounty Reports

In this article, we will discuss Remote Code Execution (RCE) vulnerability, how to find one and present 25 disclosed reports based on this issue. RCE stands for Remote Code Execution and it is a vulnerability in which an attacker can execute malicious code or commands on a target machine.

https://medium.com/@corneacristian/top-25-rce-bug-bounty-reports-bc9555cca7bc

Open Redirect using (wayback gau gosipder)

Hanno's projects disclosed on HackerOne: Open redirect on...

Summary:** There is an Open Redirect on https://blog.fuzzing-project.org/exit.php?url= due to the application not checking the value passed by the user to the "url" parameter. **Description:** Unchecked redirects occur when an application redirects to a destination controlled by attackers. This

https://hackerone.com/reports/373916

Twitter disclosed on HackerOne: XSS and Open Redirect on MoPub Login

Very simple open redirect made much more impactful by the lack of filtering javascript URIs. Thanks again to the Twitter team for a quick response/bounty!

https://hackerone.com/reports/683298

Socail-Signon Bypass

Uber disclosed on HackerOne: Authentication bypass on auth.uber.com...

subdomain takeover of saostatic.uber.com allowed for access to *.uber.com scoped SSO cookies. In response to this report, we immediately fixed the subdomain takeover and then added additional protections (IP restriction) to our *.uber.com SSO cookies to mitigate ATO possibility of subdomain

https://hackerone.com/reports/219205

Genasys Technologies disclosed on HackerOne: Ability to bypass...

Summary: An attacker is able to login to any email account (that doesn't belong to him) through using the OAuth functionality (https://staging.genasystech.co.uk/d2c-api/v1/account/login/provider) ## Steps To Reproduce: 1. Register an account with an email and verify it using the one time code that is asked upon

https://hackerone.com/reports/729960

Automattic disclosed on HackerOne: Authentication Bypass - Chaining...

Product / URL** https://en.instagram-brand.com/wp-json/brc/v1/login/ **Description and Impact** An attacker can perform account takeover by leveraging following two vulnerabilities: Auth Bypass = Username Enumeration + Login Brute Force A. Username Enumeration: ----------

https://hackerone.com/reports/209008

New Relic disclosed on HackerOne: SSO Authentication Bypass

Hi, As I reported to security@newrelic.com, here's the authentication bypass vulnerability report. I've left some details out in this report but you're welcome to reach out to me with any questions. Here's a more detailed overview: # SSO Authentication Bypass ## Summary It is possible to POST a custom SAML

https://hackerone.com/reports/168108

File Upload

leads to CSRF,SSRF,xss,LFI,XXE,RCE(fuxuploader or manual detection)

Stripo Inc disclosed on HackerOne: Unrestricted File Upload on...

Hi Stripo Inc, I found 2 Unrestricted File Upload Vulnerabilities on your website. First Vulnerability: >Step to Reproduce 1. Create an account in "https://my.stripo.email" 2. Simply Download a php shell from internet and open with text editor. ex: r57 shell 3. Then save it as JPEG file. 4.

https://hackerone.com/reports/823588

SEMrush disclosed on HackerOne: Unrestricted file upload in...

@zcashi found vulnerability in My Reports Tool.

https://hackerone.com/reports/748903

Qulture.Rocks disclosed on HackerOne: Unrestricted File Upload in...

Summary: The application allows the attacker to upload dangerous file types that can be automatically processed within the product's environment. ## Steps To Reproduce: 1. Hit the browser with below URL. https://qa.qulture.rocks/en/users/sign_in 2. Open The Cat window. 3. Upload any exe file . 4. Click on

https://hackerone.com/reports/826288

XEE Injection xml entity injection

QIWI disclosed on HackerOne: [send.qiwi.ru] Soap-based XXE...

An XML external entities injection vulnerability exists on the soap server hosted on send.qiwi.ru. The attack allows an attacker to open local files (although perhaps not return the data, see below), leading at best to a DoS.

https://hackerone.com/reports/36450

Starbucks disclosed on HackerOne: XXE at...

johnstone discovered that both ecjobs.starbucks.com.cn/retail/hxpublic_v6/hxdynamicpage6.aspx & ecjobs.starbucks.com.cn/recruitjob/hxpublic_v6/hxdynamicpage6.aspx page and were vulnerable to an XML External Entities (XXE) attack. @johnstone - thank you for reporting this vulnerability and your

https://hackerone.com/reports/500515

DuckDuckGo disclosed on HackerOne: XXE on https://duckduckgo.com

An XML External Entity (XXE) injection vulnerability was discovered in the `x.js` endpoint on https://duckduckgo.com via `u` parameter. This was due to improper sanitation of external XML entities. The results was a leak of certain world readable files on the system. This issue was patched.

https://hackerone.com/reports/483774

drchrono disclosed on HackerOne: XML Parser Bug: XXE over which...

Hello security team, I have reported this issue on Feb 6, 2015 and i'm resubmit it here again. I was able to do XXE attack on your site and exposed the /etc/passwd file. Scenario: 1. Login to drchrono site. 2. Click on patients→patient 3. Click on ' Update patient (via C-CDA XML).'

https://hackerone.com/reports/55431

Web Cache Posning

Postmates disclosed on HackerOne: Web cache poisoning attack leads...

Hello, Your Web-Server is vulnerable to web cache poisoning attacks. This means, that the attacker are able to get another user informations. If you are logged in and visit this website (For example): https://postmates.com/SomeRandomText.css Then the server will store the information in the cache,

https://hackerone.com/reports/492841

HackerOne disclosed on HackerOne: Denial of service via cache...

An attacker can persistently block access to any/all redirects on www.hackerone.com by using cache poisoning with the X-Forwarded-Port or X-Forwarded-Host headers to redirect users to an invalid port. To replicate: ```curl -H 'X-Forwarded-Port: 123' https://www.hackerone.com/index.php?

https://hackerone.com/reports/409370

Nextcloud disclosed on HackerOne: https://help.nextcloud.com::: Web...

Hi there, I just found the website: https://help.nextcloud.com is infected with "Web cache poisoning" Abuse this bug, Attacker can: 1. Poison your cache with HTTP header with XSS included. This attack may leads to Stored XSS 2. Poison your website contains malware url (cache poisoned by attacker),

https://hackerone.com/reports/429747

Bussiness Logic Error

Shopify disclosed on HackerOne: Potential to abuse pricing errors...

If someone abandons a shopping cart and the price changes between that time and when the abandoned cart recovery email is sent, the saved cart will always show the old price.

https://hackerone.com/reports/336131

HackerOne disclosed on HackerOne: Account recovery text message is...

When users setup Account recovery at Authentication section Hackerone sends them text message to their updated phone number with a wrong domain. Special thanks to @babayaga_ for helping me out. :)

https://hackerone.com/reports/549364

Inflection disclosed on HackerOne: Business Logic Flaw allowing...

Researcher misunderstood the names and permissions assigned to various roles in the GoodHire application - the permissions are working as intended. Nevertheless, the researcher requested for the report to be disclosed.

https://hackerone.com/reports/280914

Buffer overflow

Valve disclosed on HackerOne: RCE on Steam Client via buffer...

Introduction In Steam and other valve games (CSGO, Half-Life, TF2) there is a functionality to find game servers called the server browser. In order to retrieve the information about these servers the server browser communicates with a specific UDP protocol called [server queries]

https://hackerone.com/reports/470520

Liberapay disclosed on HackerOne: Buffer overflow

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of

https://hackerone.com/reports/363658

Perl (IBB) disclosed on HackerOne: Integer overflow leading to...

There exists an integer overflow in Perl_my_setenv @ util.c : 2070 2070: void Perl_my_setenv(pTHX_ const char *nam, const char *val) { ... 2166: const int nlen = strlen(nam); ... 2171: vlen = strlen(val); 2172: new_env = (char*)safesysmalloc((nlen + vlen + 2) * sizeof(char)); Here in a 64 bit version of Perl, since

https://hackerone.com/reports/424447

VLC (European Commission - DIGIT) disclosed on HackerOne: Buffer...

Summary:** When parsing an invalid AVI file, a buffer overflow might occur. **Description:** The ReadFrame function in the avi.c file uses a variable i_width_bytes, which is obtained directly from the file. It is a signed integer. It does not do a strict check before the memory operation(memmove, memcpy),

https://hackerone.com/reports/484398

Source Code Disclosure

Rockstar Games disclosed on HackerOne: Source Code Disclosure (CGI)

Hello guys. I would like to share with you my discovery. The fact is that at: > https://www.rockstargames.com/gta/game/highscores.cgi Anyone can see the source code of the script {F166966} check please Regards @d1v3r

https://hackerone.com/reports/211418

Razer disclosed on HackerOne: Source Code Disclosure

The tester discovered a PHP file with source code exposed. There was no known exploit.

https://hackerone.com/reports/819735

Mail.ru disclosed on HackerOne: Source code disclosure

PHP configuration file was available for download on few terrhq.ru subdomains

https://hackerone.com/reports/521960

Nextcloud disclosed on HackerOne: Business/Functional logic bypass:...

In nextcloud the default admin can not be removed from his admin group. The group toggle request looks like this: ``` POST /nextcloud/index.php/settings/ajax/togglegroups.php HTTP/1.1 Host: 139.59.9.184 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0

https://hackerone.com/reports/145745

Information disclosure

Vanilla disclosed on HackerOne: Forum Users Information Disclosure

Summary:** An unauthorized (even unauthenticated) user is able to view some private information about forum users. this information includes: email address (even if the user not allows it), IP address of the user, data of some of the private messages between two users.

https://hackerone.com/reports/321249

Uber disclosed on HackerOne: Sensitive user information disclosure...

It was possible for an attacker to insert another user's UUID into the userUuid POST parameter when making a request to https://bonjour.uber.com/marketplace/_rpc?rpc=getConsentScreenDetails, allowing them to retrieve personal data from the victim user's account, as well as the user's mobile auth token,

https://hackerone.com/reports/542340

Web-cache deception

Chaturbate disclosed on HackerOne: Web cache deception attack -...

Hello, I have found new Vulnerability in your website which called Web cache deception attack. It's found first time in Paypal. ###Web Cache Deception Attack Websites often tend to use web cache functionality to store files that are often retrieved, to reduce latency from the web server.

https://hackerone.com/reports/397508

SEMrush disclosed on HackerOne: Web cache deception attack - expose...

Hello, I have found new Vulnerability in your website which called Web cache deception attack. It's found first time in Paypal. ###Web Cache Deception Attack Websites often tend to use web cache functionality to store files that are often retrieved, to reduce latency from the web server.

https://hackerone.com/reports/439021

RACE CONDITIONS

Top 25 Race Condition Bug Bounty Reports

In this article, we will discuss Race Condition vulnerability, how to find one, and present 25 disclosed reports based on this issue. According to OWASP: "A race condition is a flaw that produces an unexpected result when the timing of actions impact other actions.

https://medium.com/@corneacristian/top-25-race-condition-bug-bounty-reports-84f9073bf9e5

APPLICATION LOGIC AND CONFIGURATION VULNERABILITIES

Penetrating Pays: The Pornhub Story

Currently at time of writing I'm ranked #1 finder of Bugs on https://hackerone.com/pornhub which is a nice position to hold. This post is to explain the techniques I've used to get to where I am and how I found my most recent $2500 bug on pornhub.

https://blog.zsec.uk/pwning-pornhub/

HackerOne disclosed on HackerOne: AWS S3 bucket writeable for...

An ACL misconfiguration issue existed on one of our S3 buckets. This misconfiguration allowed any authenticated AWS user to write to this bucket (no read access was permitted). An attacker could theoretically post a file into that bucket that may at some point be accessed by a HackerOne staff

https://hackerone.com/reports/128088/

[BugBounty] Yahoo phpinfo.php disclosure

Dear readers, during my research of yahoo i found a phpinfo.php file information disclosure vulnerability, on one of their servers. The server on which i found that particular file was : http://nc10.n9323.mail.ne1.yahoo.com/phpinfo.php you might ask yourself how on earth i found this

https://blog.it-securityguard.com/bugbounty-yahoo-phpinfo-php-disclosure-2/

HackerOne disclosed on HackerOne: Inadequate access controls in...

Hello there, First of all let me congratulate you for including pornhub in the list of bug bounty programs, me and my colleagues will have a lot of fun with it hahahahahah. Awesome... Anyways, I stumbled upon something whilst testing hackerone's main site.

https://hackerone.com/reports/137503/

GitLab disclosed on HackerOne: Bypassing password authentication of...

This vulnerability allowed password authentication to be bypassed when two-factor authentication was enabled for a user. @GitLab resolved this 2 days after I reported it to them. The commit that fixed the bug can be found at https://gitlab.com/gitlab-org/gitlab-

https://hackerone.com/reports/128085/

Shopify disclosed on HackerOne: An administrator without any...

Description** ---- An administrator who lacks the 'Settings' permission is not able to add notifications through the UI. But the endpoint `shop.myshopify.com/admin/mobile_devices.json` does allow the unprivileged user to add his own device. **PoC** ---- This PoC simply show how to get & re-use the

https://hackerone.com/reports/100938/

HackerOne disclosed on HackerOne: Improve signals in reputation

New section has been added recently in reputation where you can see something called as signal , which says average reputation per report. However, you can improve your signal points by following below steps Steps: create any report in any team self close the bug see your signal in reputation.

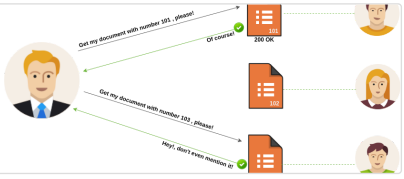
https://hackerone.com/reports/106305

IDOR

Top 25 IDOR Bug Bounty Reports

In this article, we will discuss IDOR vulnerability, how to find one and present 25 disclosed reports based on this issue. IDOR stands for Insecure Direct Object Reference and it is a vulnerability in which an attacker can access sensitive information by making unauthorized references.

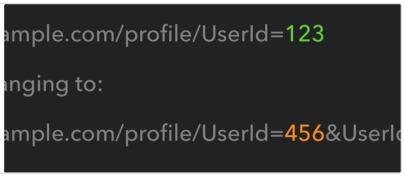
https://medium.com/@corneacristian/top-25-idor-bug-bounty-reports-ba8cd59ad331



[Case Study] Bypassing IDOR via Parameter Pollution

While working on a pentest engagement, I found an interesting IDOR (Insecure Direct Object Reference) bypass using parameter pollution (a much overlooked test case). I was looking out for the IDOR vulnerabilities within the REST-API of the target application. Unfortunately, none of the endpoints

https://medium.com/@0xgaurang/case-study-bypassing-idor-via-parameter-pollution-78f7b3f9f59d



Cheak for State Parameter in Social-in & Cheak whether it,s Possible to cause Dos Using cookie injection

Session Fixation

GraphQL

Tool

inql

[!] Remote GraphQL Endpoint OR a Schema file in JSON format must be specified!

CRLF

Tool

Use BRUP

or

crlf scanner

Command Injection

command injection are as
follows:
Cookies
X-Forwarded-For
User-Agent
Referrer