Bug Bounty

Khael Kugler

I am always

TWO BUGS AHEAD

989 Chick-fil-A Spicy Deluxe Chicken Sandwiches (with Pepperjack Cheese)

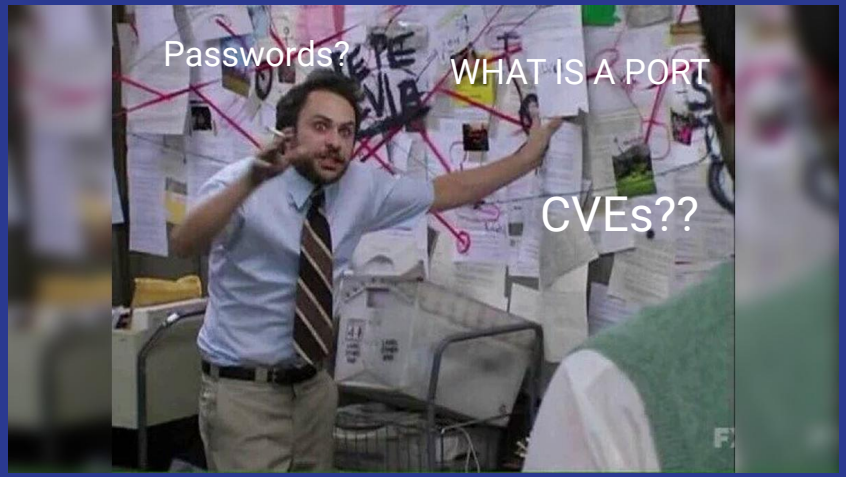
← 989????

989 Chick-fil-A Spicy Deluxe Chicken Sandwiches (with Pepperjack Cheese)?????

(Did you attend the wrong talk?)

(probably)

How????



MONEY

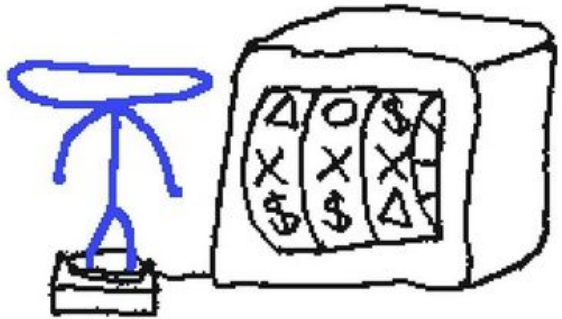
$4.27 billion (I’m not kidding)

UT’s annual budget

UT’s annual security budget
(enlarged)

The 3-step Get Rich Quick ~~Scheme~~ Technique:

1. Scope UT’s infrastructure
2. Investigate said infrastructure
3. Hack said infrastructure



1. Scoping out UT’s Infrastructure

What is actually in-scope?

hackerone

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
146.6.0.0/16	CIDR	In scope	High	Eligible	Apr 8, 2022	0 (0%)
172.16.0.0/12	CIDR	In scope	High	Eligible	Apr 8, 2022	0 (0%)
10.0.0.0/8	CIDR	In scope	High	Eligible	Apr 8, 2022	0 (0%)
129.116.0.0/16	CIDR	In scope	High	Eligible	Apr 8, 2022	0 (0%)
128.83.0.0/16	CIDR	In scope	High	Eligible	Apr 8, 2022	0 (0%)
*.utexas.edu	Wildcard	In scope	High	Eligible	May 15, 2023	161 (101%)
*.utdirect.utexas.edu	Wildcard	Out of scope	None	Ineligible	Mar 14, 2024	0 (0%)

146.16.0.0 -> 146.6.255.255

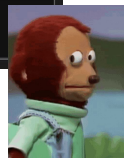
172.16.0.0 -> 172.31.255.255

10.0.0.0 -> 10.255.255.255

129.116.0.0 -> 129.116.255.255

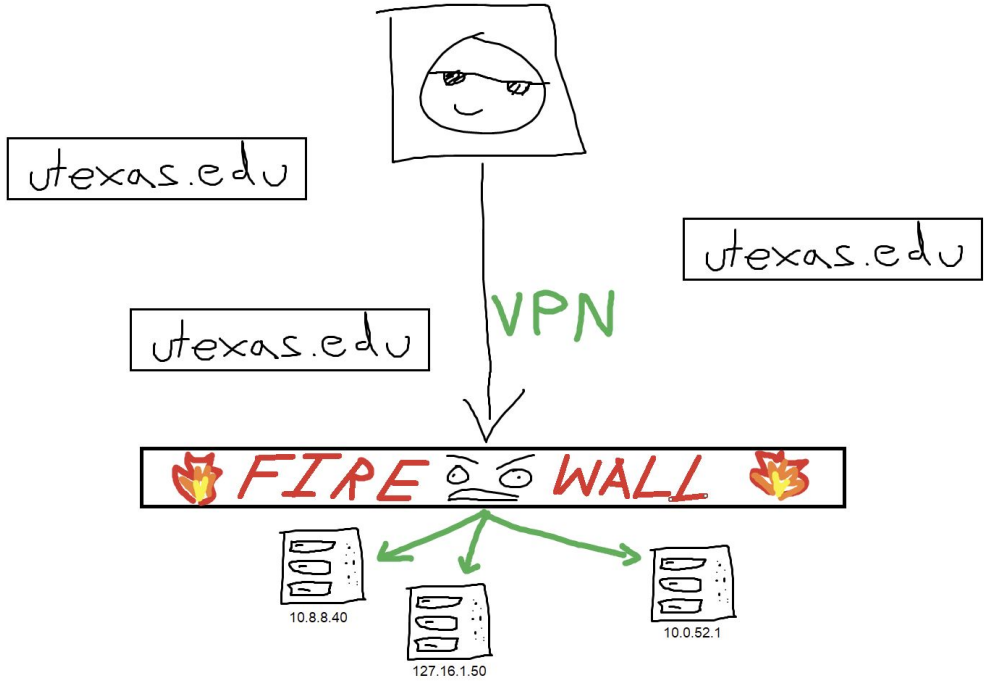
129.116.0.0 -> 129.116.255.255

{anything}.utexas.edu



But how am I supposed to access internal IPs?

The UT VPN allows you to get past the firewall and into the internal UT network



And how can I enumerate these IP ranges?

NMAP!!

- This tool is your best friend once on the UT VPN

Enumerating these IP ranges and searching for ports

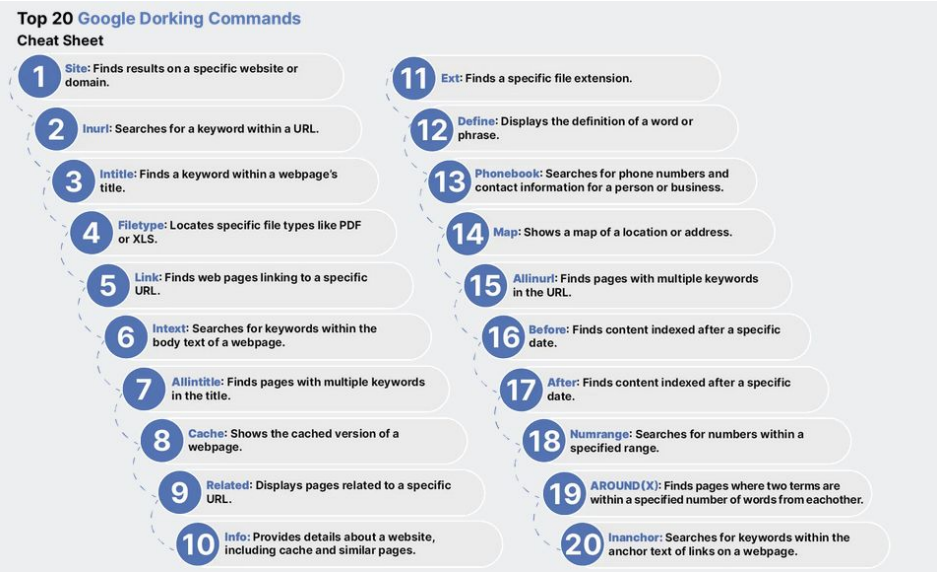
- `nmap 172.16.0.0/16 –p 80,443,8000,8080,8443`
  - Checks for the most commonly open web ports coming from any 172.16.x.x IP

Scoping external websites

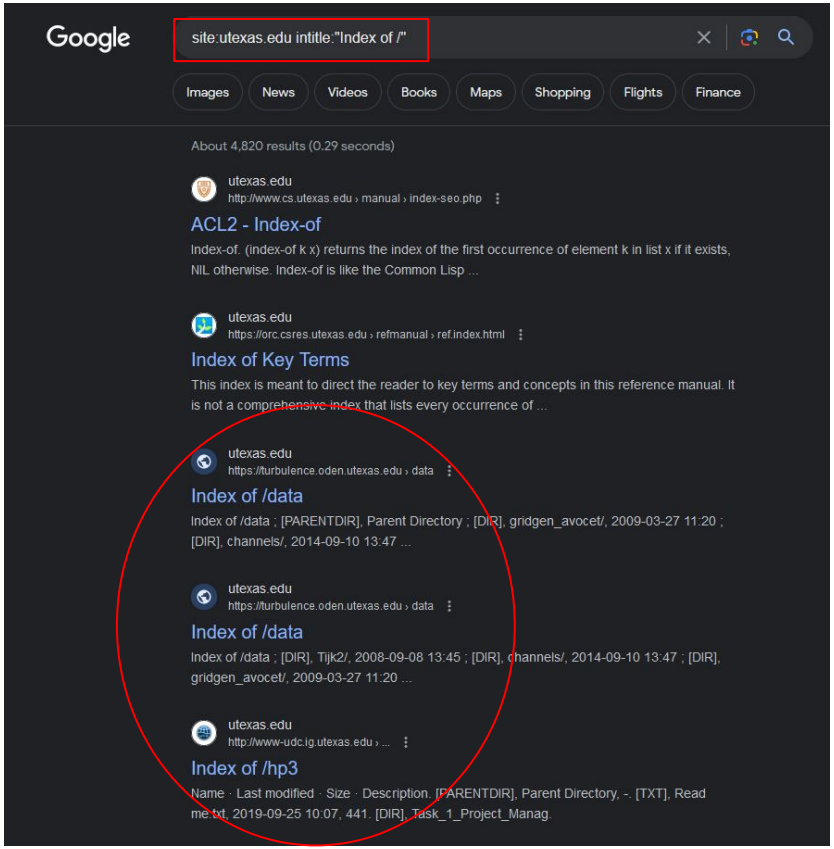
- Google Dorking
  - Searching for insecure sites indexed by Google
  - Very, very, (very) useful
- Exploring feature-rich webpages
  - Sites with lots of functionality, like the UT RecSports page or library pages
  - The attack surface is large, giving more chances for cracks
- Compiling a list of ALL webservers
  - https://khaelkugler.com/misc/subdomains.html
  - I used crt.sh to compile a list of thousands of UT subdomains, which were then checked for a website

Google dorking utexas.edu

- Search for PDFs with passwords!
  - Filetype:pdf site:utexas.edu intext:password
- Search for admin PHP pages!
  - Filetype:php site:utexas.edu inurl:admin
- Search for outdated software!
  - Intext:"Apache/2.2.15" site:utexas.edu
- There are tons of resources giving good dorking payloads
  - “Top 20 Google Dork Payloads” is great



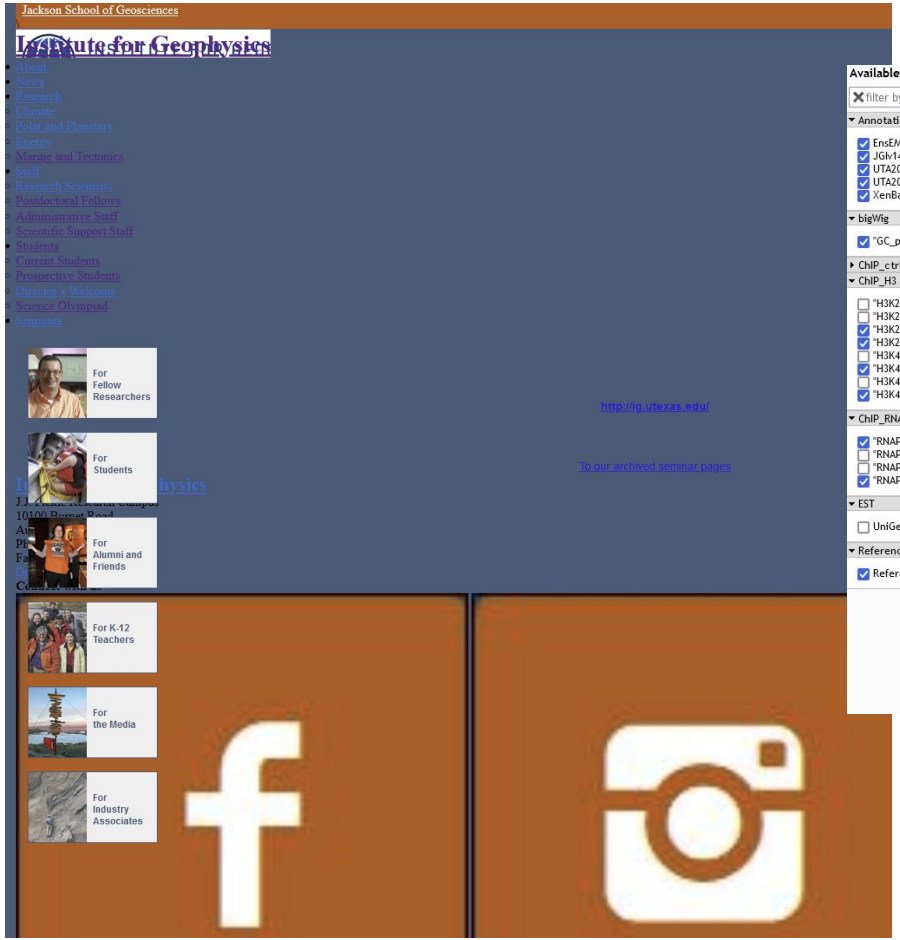
The possibilities are
E N D L E S S

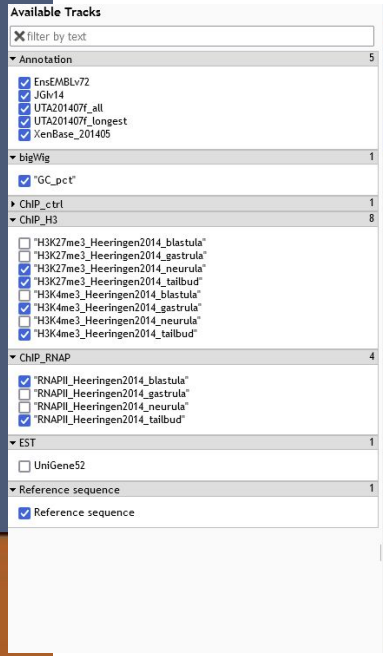


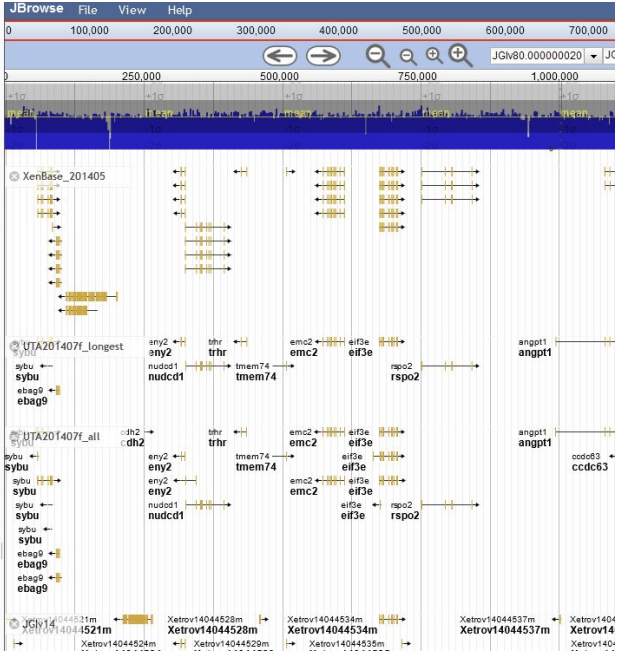
Index of /

Name↓	Last Modified:	Size:	Type:
ALMNH/	2020-Dec-01 12:21:32	-	Directory
Blanton/	2016-Nov-10 14:01:10	-	Directory
CAS/	2020-Jul-16 13:39:36	-	Directory
field/	2018-Mar-28 05:02:35	-	Directory
GSAF/	2016-Dec-06 19:56:07	-	Directory
ICA/	2017-Jan-25 13:26:38	-	Directory
irods-web/	2017-May-19 16:17:53	-	Directory
isobank/	2021-Jul-01 16:13:20	-	Directory
KNewman/	2016-Nov-13 06:44:58	-	Directory
MDACC-DIP/	2016-Nov-16 20:25:29	-	Directory
MOST/	2017-Oct-04 00:25:16	-	Directory
MSB/	2016-Nov-16 16:56:23	-	Directory
MVZ/	2020-Mar-20 15:54:35	-	Directory
OneKP/	2016-Nov-14 03:33:26	-	Directory
oplontis/	2019-Jun-16 20:39:17	-	Directory
PetroSpect/	2017-Jan-25 14:29:26	-	Directory
sharing/	2020-Dec-04 15:39:30	-	Directory
Texas_Politics/	2017-Jan-25 14:30:12	-	Directory
TNSC/	2016-Nov-22 14:30:01	-	Directory
TWDL/	2016-Nov-18 15:29:29	-	Directory
UAF/	2018-Mar-05 17:00:28	-	Directory
UCM/	2021-Jul-14 15:27:16	-	Directory
UTEP/	2017-Dec-05 14:21:45	-	Directory
UWBM/	2020-Mar-20 15:48:28	-	Directory
UWYMV/	2018-May-22 12:55:25	-	Directory
XALT/	2017-Jan-06 15:03:29	-	Directory

lighttpd/1.4.55


Jackson School of Geosciences
Institute for Geophysics
About
News
Research
Climate
Polar and Planetary
Energy
Marine and Tectonics
Staff
Research Scientists
Postdoctoral Fellows
Administrative Staff
Scientific Support Staff
Students
Current Students
Prospective Students
Director's Welcome
Science Olympiad
Seminars
For Fellow Researchers
For Students
For Alumni and Friends
For K-12 Teachers
For the Media
For Industry Associates
http://ig.utexas.edu/
To our archived seminar pages

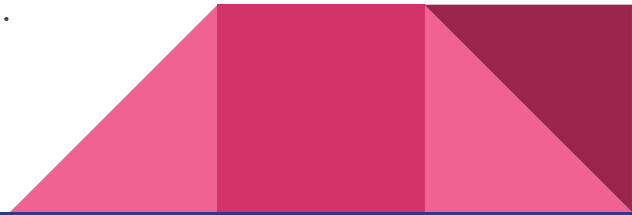

Available Tracks
filter by text
Annotation 5
EnsEMBLv72
JGIv14
UTA201407f_all
UTA201407f_longest
XenBase_201405
bigWig 1
"GC_pct"
ChIP_ctrl 1
ChIP_H3 8
"H3K27me3_Heeringen2014_blastula"
"H3K27me3_Heeringen2014_gastrula"
"H3K27me3_Heeringen2014_neurula"
"H3K27me3_Heeringen2014_tailbud"
"H3K4me3_Heeringen2014_blastula"
"H3K4me3_Heeringen2014_gastrula"
"H3K4me3_Heeringen2014_neurula"
"H3K4me3_Heeringen2014_tailbud"
ChIP_RNAP 4
"RNAPII_Heeringen2014_blastula"
"RNAPII_Heeringen2014_gastrula"
"RNAPII_Heeringen2014_neurula"
"RNAPII_Heeringen2014_tailbud"
EST 1
UniGene52
Reference sequence 1
Reference sequence


JBrowse File View Help
XenBase_201405
UTA201407f_longest
UTA201407f_all
JGIv14
sybu
ebag9
nudcd1
tmem74
emc2
eif3e
rspo2
angpt1
ccdc63
Xetrov14044521m
Xetrov14044528m
Xetrov14044534m
Xetrov14044537m

2. Investigating the Infrastructure

What to look for in a webpage

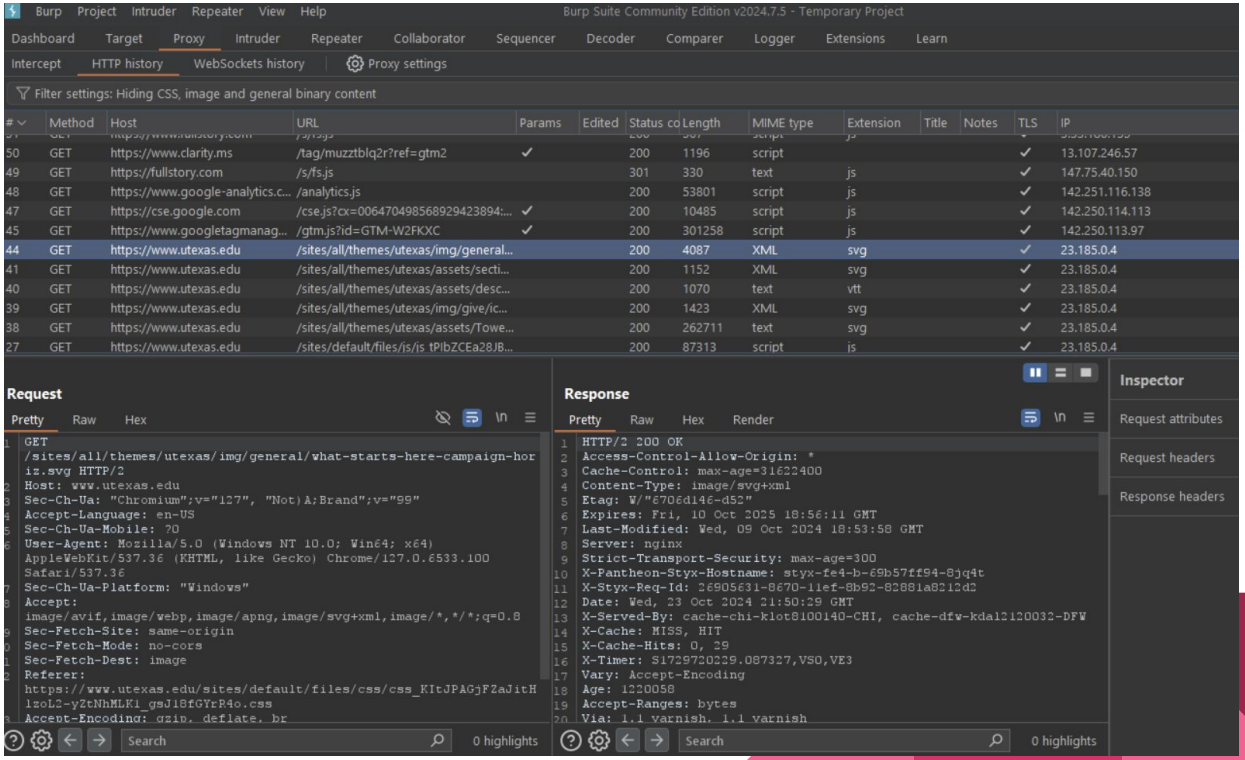
- Any and every source of user input
  - In these fields, I like to put the string `..//'"</>${};`
  - See what breaks
- Odd/custom functionality
  - Generally, templated UT pages are pretty static and boring
- Outdated software (e.g. really old Apache/Wordpress)
  - There are usually premade exploits out there (cvedetails.com)
- Login fields
  - If you find a 3rd party login page, lookup the default credentials. Also just try admin/admin, admin/password, root/root, and other common combinations.
- Administrative/configuration pages



3. Hacking UT’s Infrastructure

Modifying Web Requests - Burp Suite

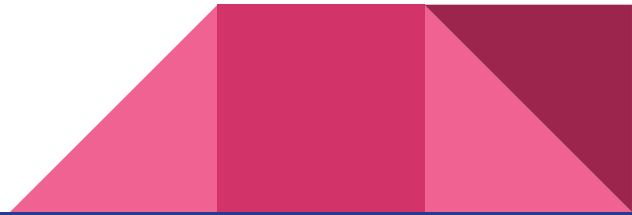
- Free!
- Used to catch and replay HTTP traffic
- Has an ez-use built in browser
- Has other awesome features



You’ve already learned about common web vulns

You just gotta apply them! The most common vulns I’ve found on UT are:

- XSS. It’s everywhere. Literally everywhere.
- Default/weak credentials
- SQL injection
  - Less common, but surprisingly still around
- File upload vulnerabilities
  - Upload malicious HTML pages with XSS! Upload webshells! Overwrite other files!



A side note: UT’s Wiki

The UT Wiki is a gold mine. An actual, real life infinite money glitch.

Searching for “password” is a big one, but other things like “AsPlainText”, “Authorization: Basic”, “root”, “ssh”, “passwd”, “logins” will also work

Look around, try to find stuff you shouldn’t see

UT Bug Bounty

What you'll look for

Find all kinds of bugs on UT's domains

- Cross-site scripting (XSS) $$$
- SQL injection
- Weak/default passwords
- File upload vulnerabilities
- Authorization bypass/escalation
- Sensitive information leaks

What you won't do

- Run automated scans like Nessus
- Leak sensitive data
- Completely ruin things
- Mess with regular business operations
- Run ANY TESTING off of the UT VPN
- Share the vulnerabilities you find

Wanna get started?

Just search "UT Bug Bounty"

Thanks! Questions???

Email: khael.kugler@praetorian.com
Discord: @malfuncti0nal