Pentest CMD Manager

NOZES

whoami

Cooler, just another computer coder...

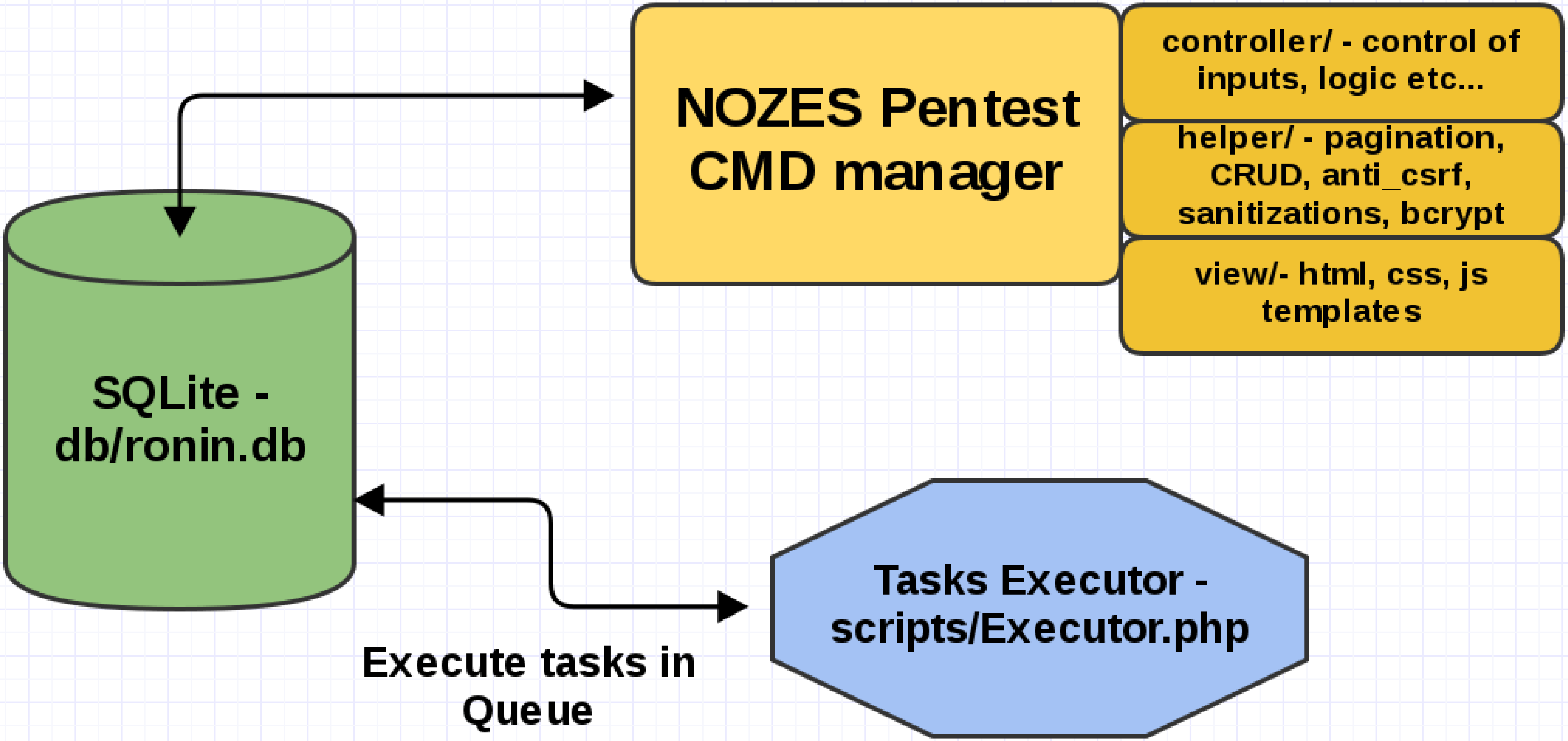
https://github.com/CoolerVoid/

NOZES

Motivations

* Gain time in Pentest.
* Result control.
* Control of attacks.
* Automate commands.
* Customize attacks.
* Optimize your work.

Flow view



NOZES Pentest CMD manager

controller/ - control of inputs, logic etc...

helper/ - pagination, CRUD, anti_csrf, sanitizations, bcrypt

view/- html, css, js templates

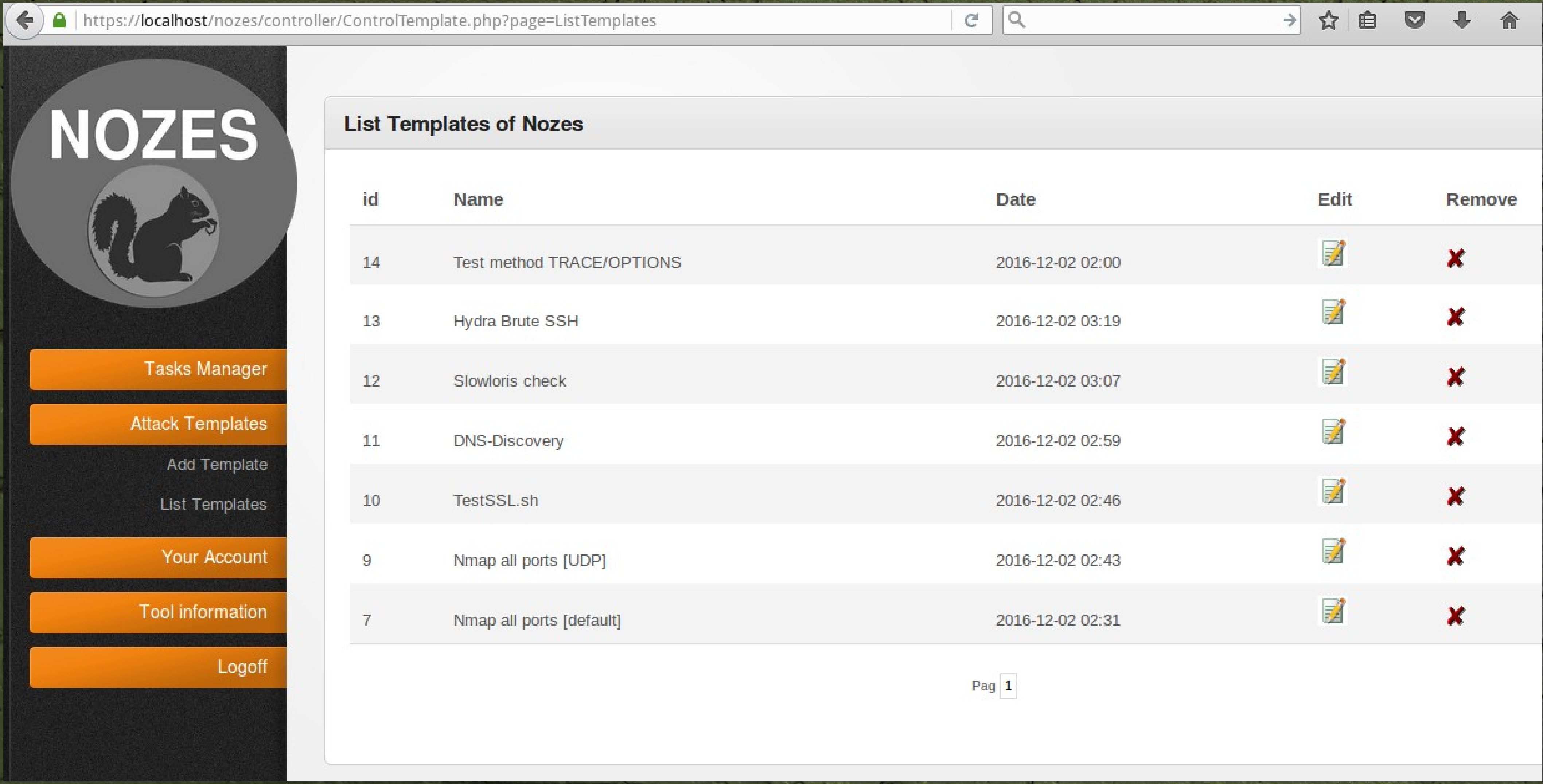
SQLite - db/ronin.db

Tasks Executor - scripts/Executor.php

Execute tasks in Queue

NOZES

view



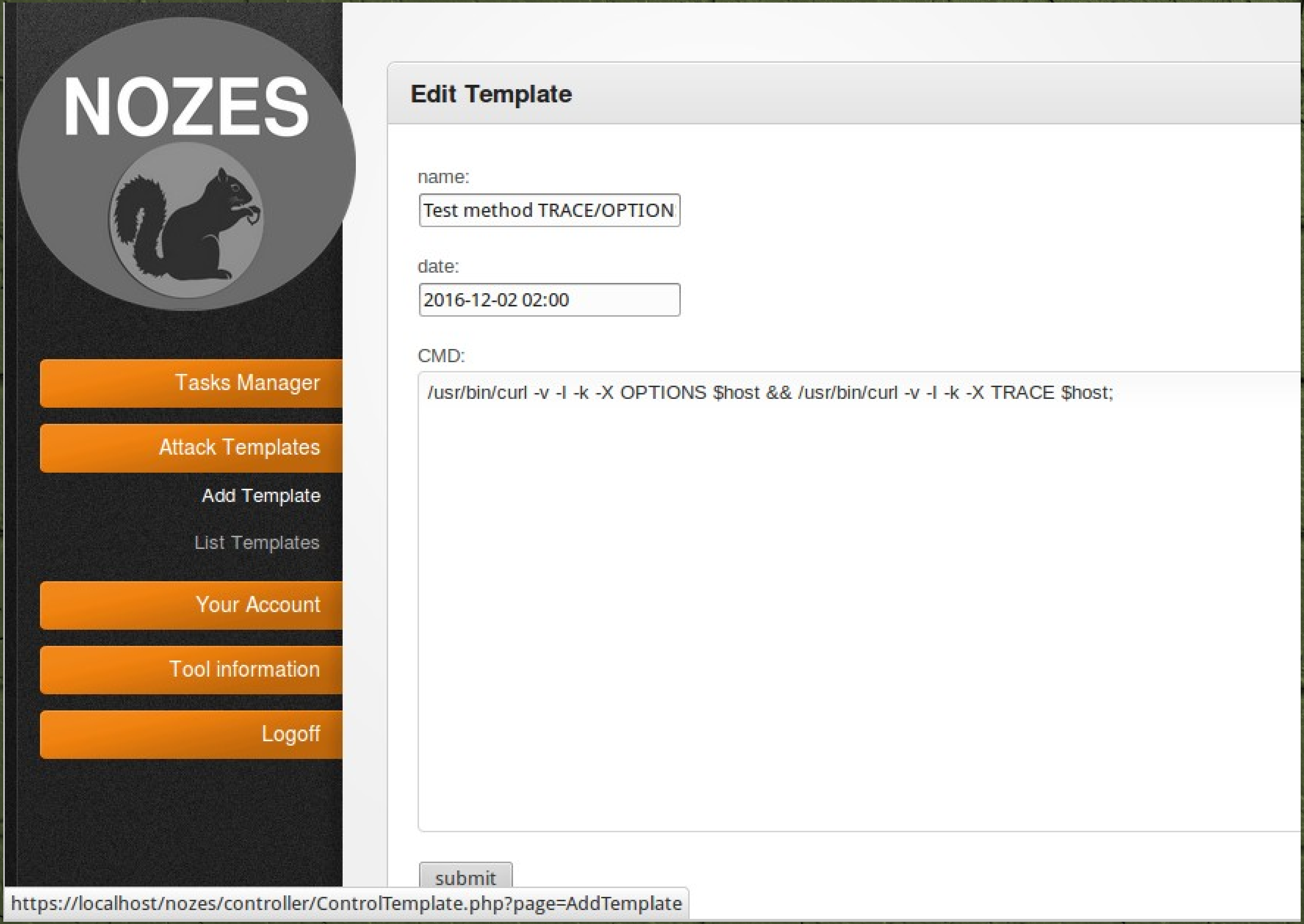
https://localhost/nozes/controller/ControlTemplate.php?page=ListTemplates

List Templates of Nozes

id	Name	Date	Edit	Remove
14	Test method TRACE/OPTIONS	2016-12-02 02:00	✎	✘
13	Hydra Brute SSH	2016-12-02 03:19	✎	✘
12	Slowloris check	2016-12-02 03:07	✎	✘
11	DNS-Discovery	2016-12-02 02:59	✎	✘
10	TestSSL.sh	2016-12-02 02:46	✎	✘
9	Nmap all ports [UDP]	2016-12-02 02:43	✎	✘
7	Nmap all ports [default]	2016-12-02 02:31	✎	✘

Pag 1

View – macros $var



Edit Template

name:
Test method TRACE/OPTION

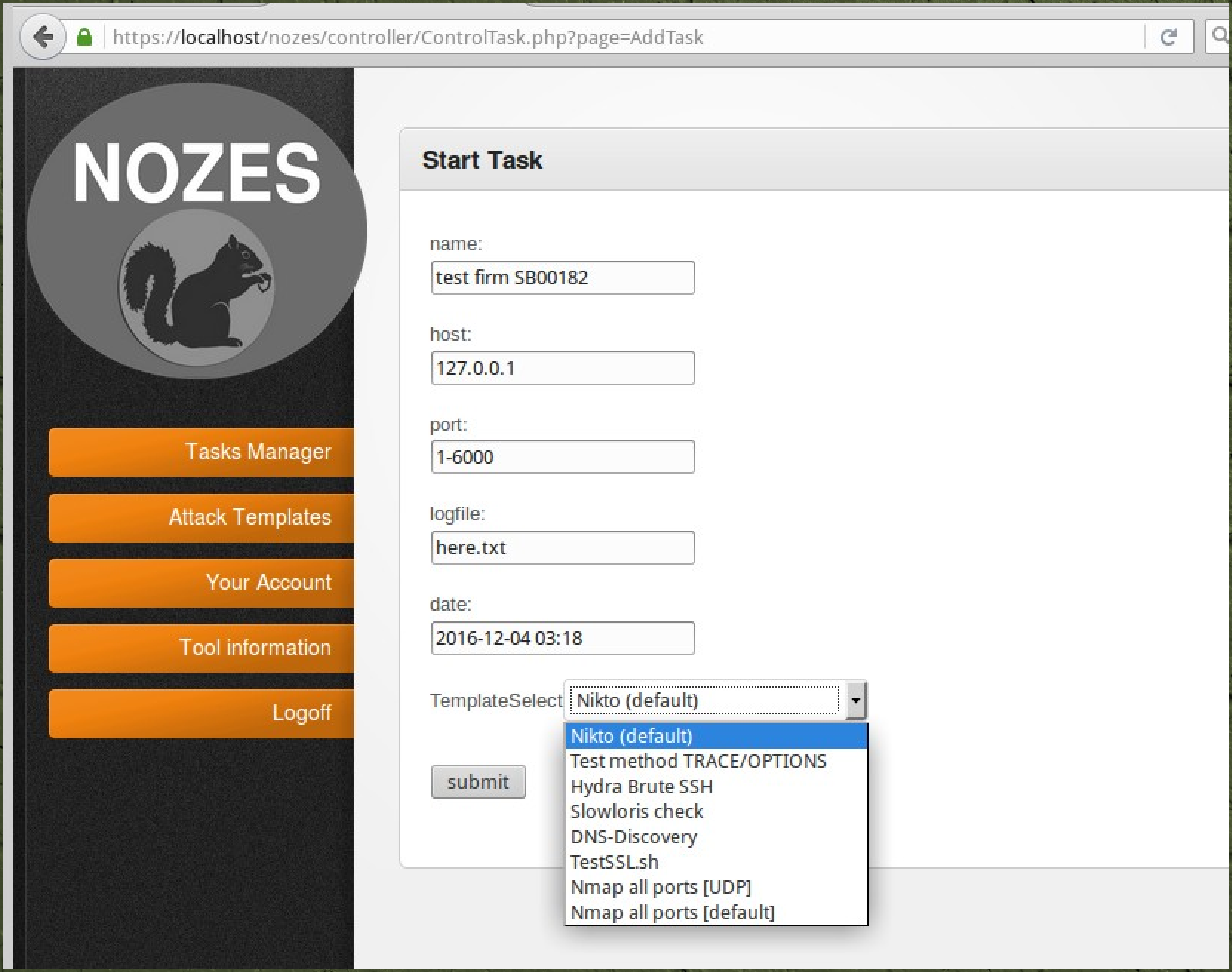
date:
2016-12-02 02:00

CMD:

```
/usr/bin/curl -v -I -k -X OPTIONS $host && /usr/bin/curl -v -I -k -X TRACE $host;
```

https://localhost/nozes/controller/ControlTemplate.php?page=AddTemplate

view



Start Task

name: test firm SB00182

host: 127.0.0.1

port: 1-6000

logfile: here.txt

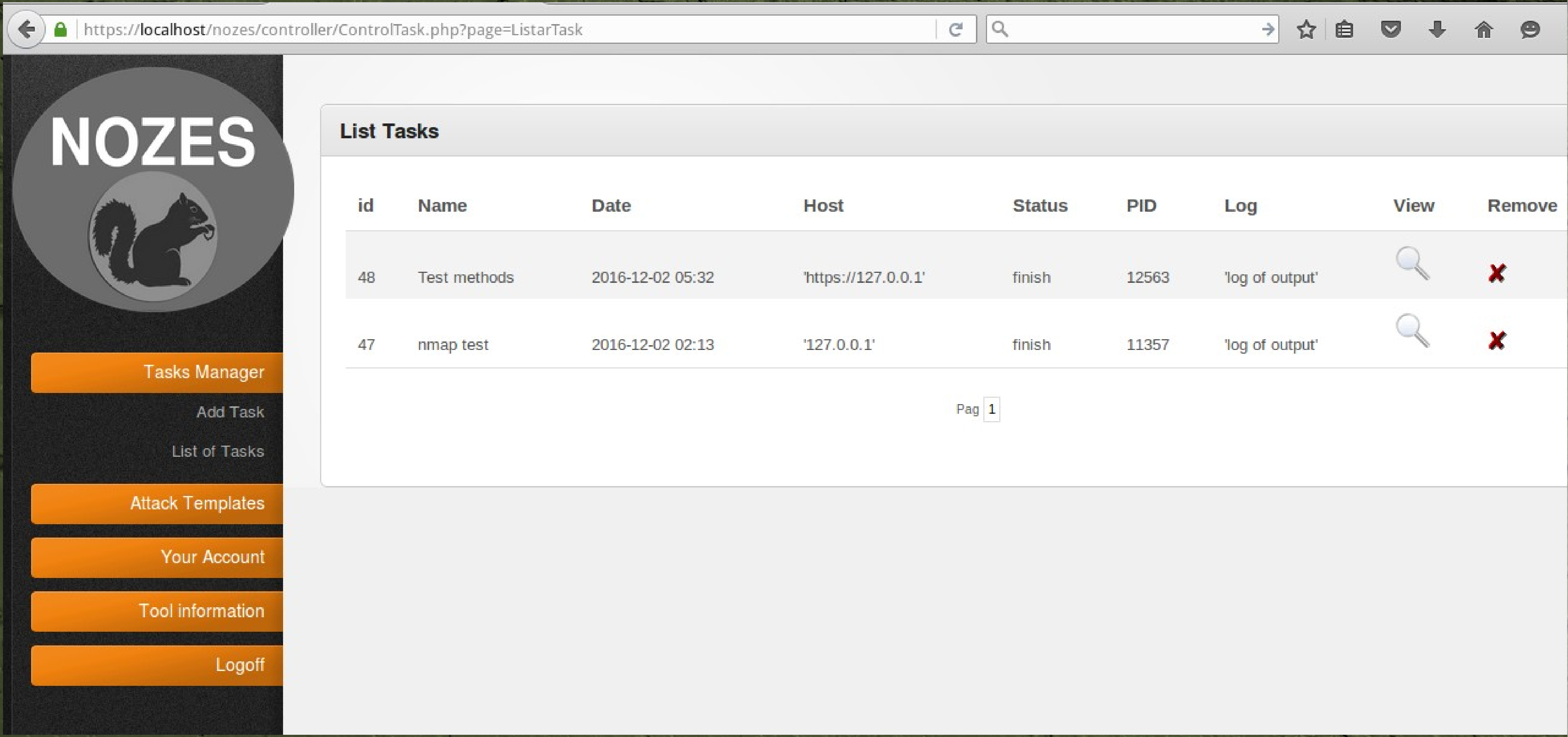
date: 2016-12-04 03:18

TemplateSelect: Nikto (default)

- Nikto (default)
- Test method TRACE/OPTIONS
- Hydra Brute SSH
- Slowloris check
- DNS-Discovery
- TestSSL.sh
- Nmap all ports [UDP]
- Nmap all ports [default]

NOZES

view



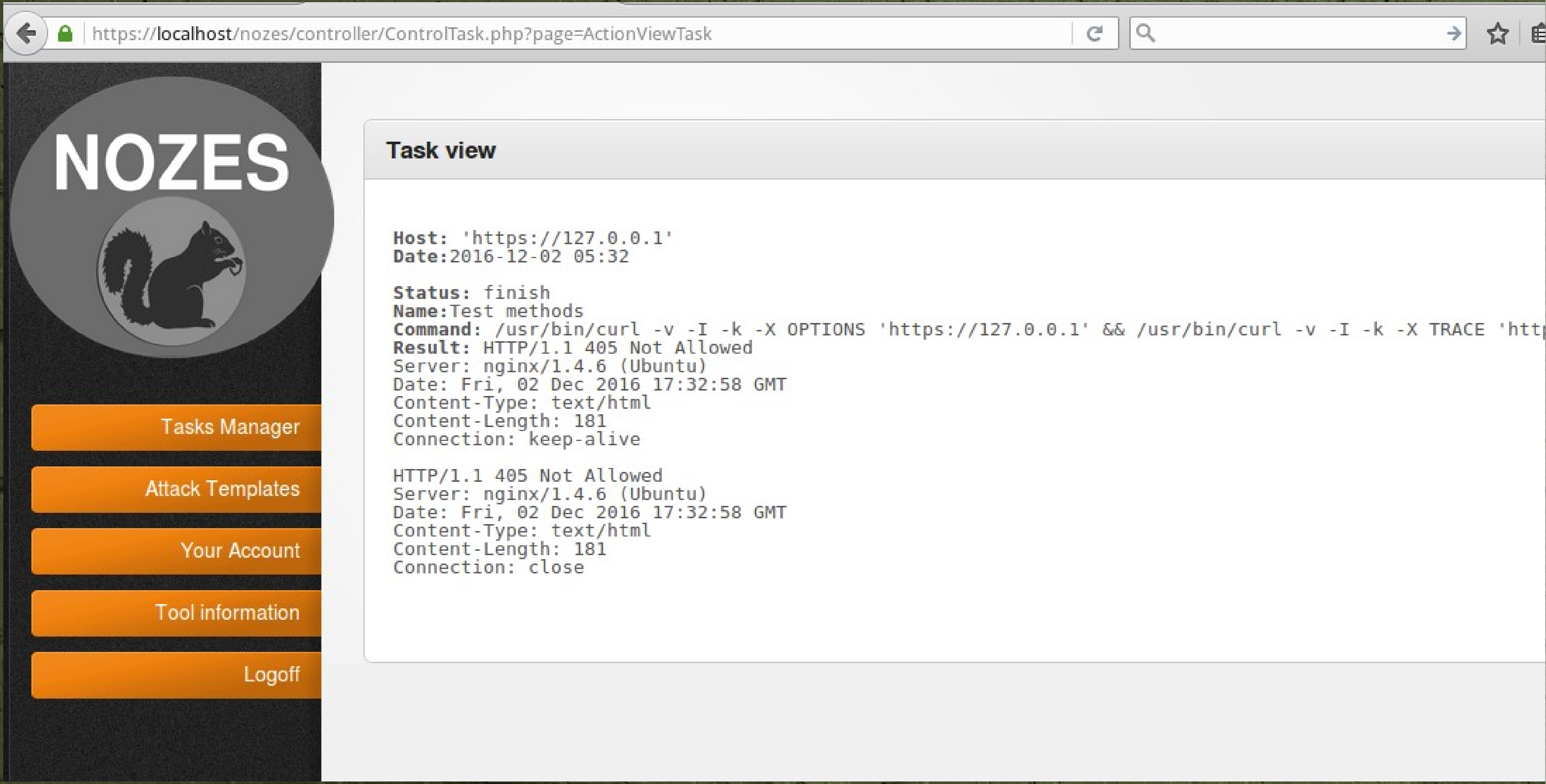
https://localhost/nozes/controller/ControlTask.php?page=ListarTask

List Tasks

id	Name	Date	Host	Status	PID	Log	View	Remove
48	Test methods	2016-12-02 05:32	'https://127.0.0.1'	finish	12563	'log of output'	🔍	✘
47	nmap test	2016-12-02 02:13	'127.0.0.1'	finish	11357	'log of output'	🔍	✘

Pag 1

view

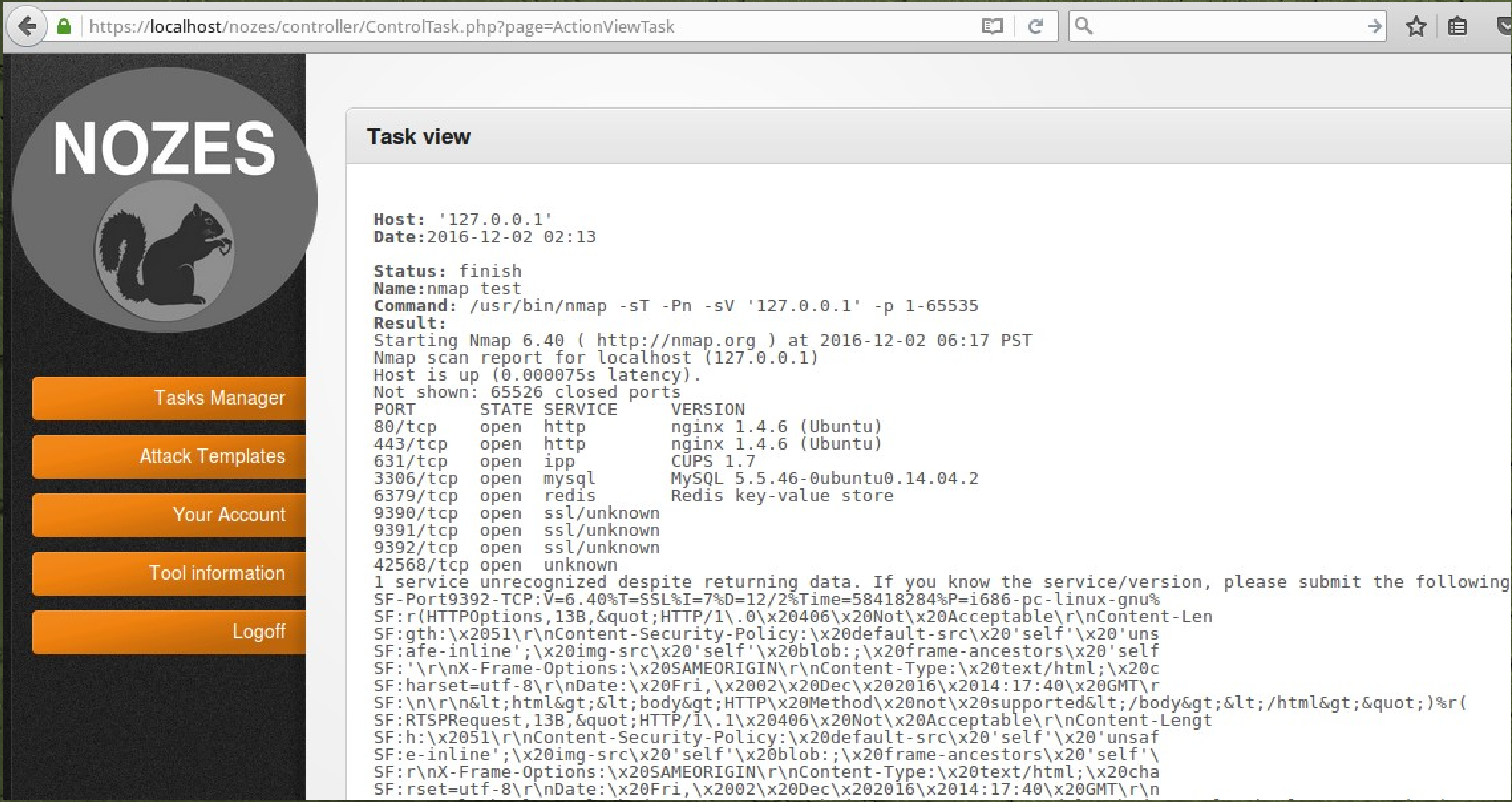


https://localhost/nozes/controller/ControlTask.php?page=ActionViewTask
NOZES
Tasks Manager
Attack Templates
Your Account
Tool information
Logoff

Task view

```
Host: 'https://127.0.0.1'
Date:2016-12-02 05:32

Status: finish
Name:Test methods
Command: /usr/bin/curl -v -I -k -X OPTIONS 'https://127.0.0.1' && /usr/bin/curl -v -I -k -X TRACE 'htt
Result: HTTP/1.1 405 Not Allowed
Server: nginx/1.4.6 (Ubuntu)
Date: Fri, 02 Dec 2016 17:32:58 GMT
Content-Type: text/html
Content-Length: 181
Connection: keep-alive

HTTP/1.1 405 Not Allowed
Server: nginx/1.4.6 (Ubuntu)
Date: Fri, 02 Dec 2016 17:32:58 GMT
Content-Type: text/html
Content-Length: 181
Connection: close
```

view



https://localhost/nozes/controller/ControlTask.php?page=ActionViewTask
NOZES
Tasks Manager
Attack Templates
Your Account
Tool information
Logoff

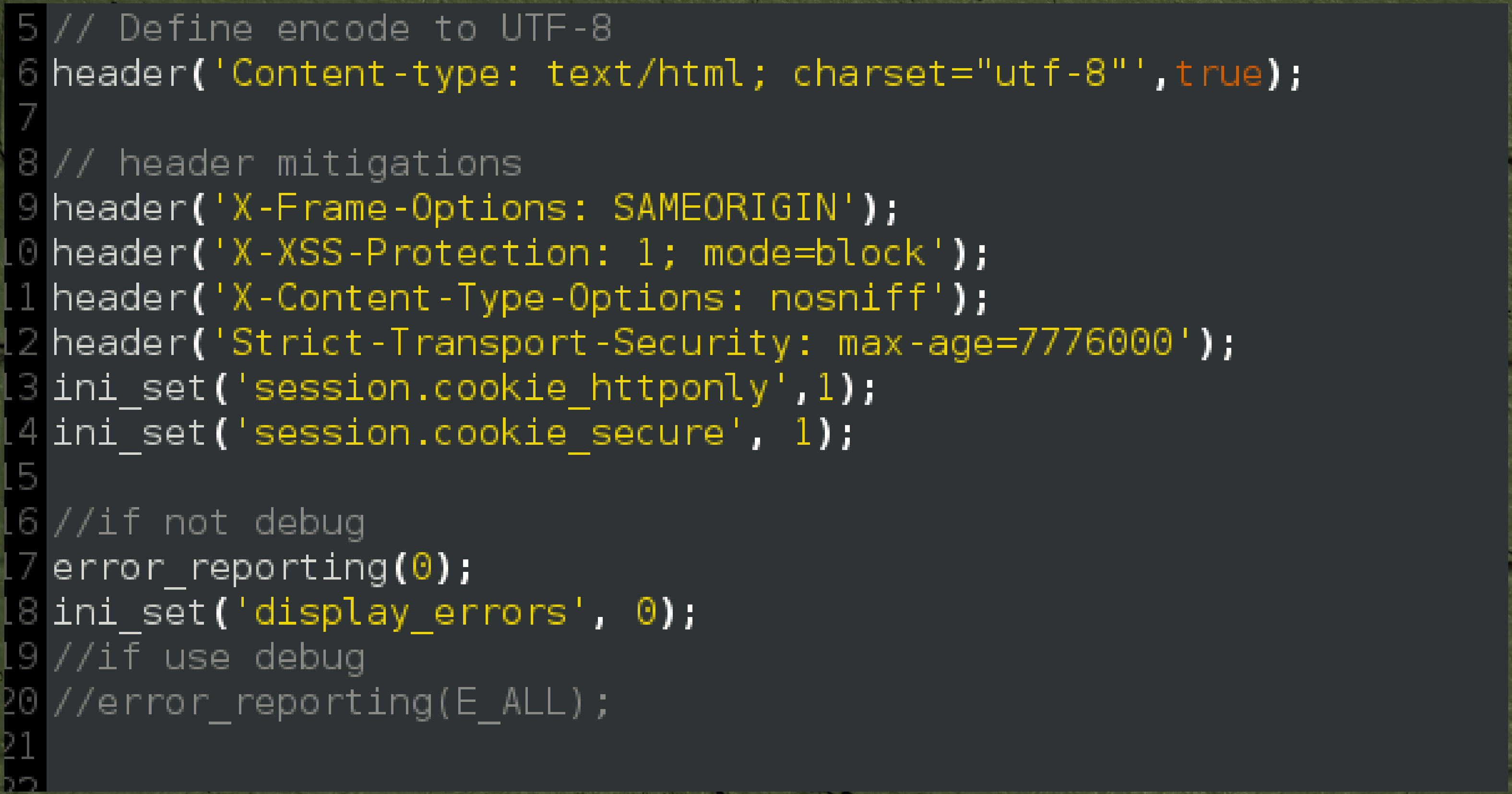
Task view

```
Host: '127.0.0.1'
Date:2016-12-02 02:13

Status: finish
Name:nmap test
Command: /usr/bin/nmap -sT -Pn -sV '127.0.0.1' -p 1-65535
Result:
Starting Nmap 6.40 ( http://nmap.org ) at 2016-12-02 06:17 PST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000075s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        nginx 1.4.6 (Ubuntu)
443/tcp   open  http        nginx 1.4.6 (Ubuntu)
631/tcp   open  ipp         CUPS 1.7
3306/tcp  open  mysql       MySQL 5.5.46-0ubuntu0.14.04.2
6379/tcp  open  redis       Redis key-value store
9390/tcp  open  ssl/unknown
9391/tcp  open  ssl/unknown
9392/tcp  open  ssl/unknown
42568/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following
SF-Port9392-TCP:V=6.40%T=SSL%I=7%D=12/2%Time=58418284%P=i686-pc-linux-gnu%
SF:r(HTTPOptions,13B,&quot;HTTP/1\.0\x20406\x20Not\x20Acceptable\r\nContent-Len
SF:gth:\x2051\r\nContent-Security-Policy:\x20default-src\x20'self'\x20'uns
SF:afe-inline';\x20img-src\x20'self'\x20blob:;\x20frame-ancestors\x20'self
SF:'\r\nX-Frame-Options:\x20SAMEORIGIN\r\nContent-Type:\x20text/html;\x20c
SF:harset=utf-8\r\nDate:\x20Fri,\x2002\x20Dec\x202016\x2014:17:40\x20GMT\r
SF:\n\r\n&lt;html&gt;&lt;body&gt;HTTP\x20Method\x20not\x20supported&lt;/body&gt;&lt;/html&gt;&quot;)%r(
SF:RTSPRequest,13B,&quot;HTTP/1\.1\x20406\x20Not\x20Acceptable\r\nContent-Lengt
SF:h:\x2051\r\nContent-Security-Policy:\x20default-src\x20'self'\x20'unsaf
SF:e-inline';\x20img-src\x20'self'\x20blob:;\x20frame-ancestors\x20'self'\
SF:r\nX-Frame-Options:\x20SAMEORIGIN\r\nContent-Type:\x20text/html;\x20cha
SF:rset=utf-8\r\nDate:\x20Fri,\x2002\x20Dec\x202016\x2014:17:40\x20GMT\r\n
```

NOZES

Hardening headers

nozes/controller/boot.php

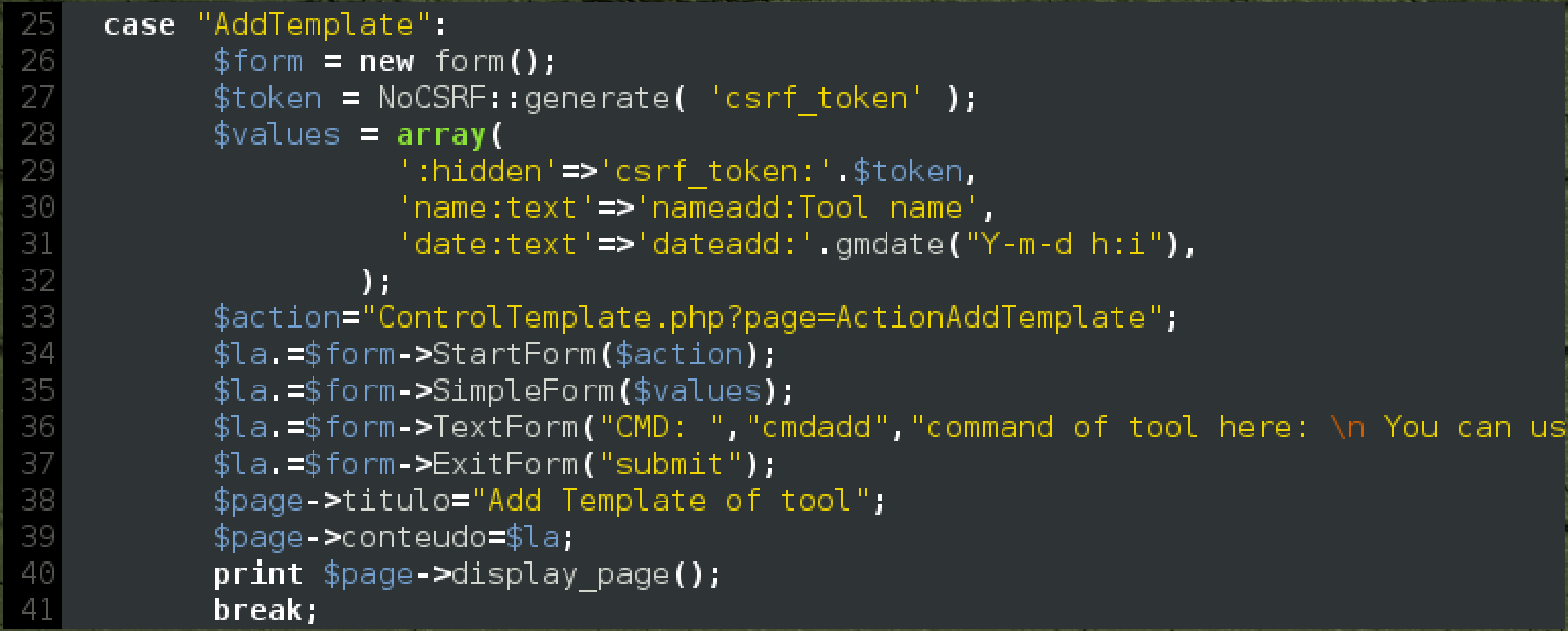


```
// Define encode to UTF-8
header('Content-type: text/html; charset="utf-8"',true);

// header mitigations
header('X-Frame-Options: SAMEORIGIN');
header('X-XSS-Protection: 1; mode=block');
header('X-Content-Type-Options: nosniff');
header('Strict-Transport-Security: max-age=7776000');
ini_set('session.cookie_httponly',1);
ini_set('session.cookie_secure', 1);

//if not debug
error_reporting(0);
ini_set('display_errors', 0);
//if use debug
//error_reporting(E_ALL);

```

NOZES

Simple code

nozes/controller/ControlTemplate.php

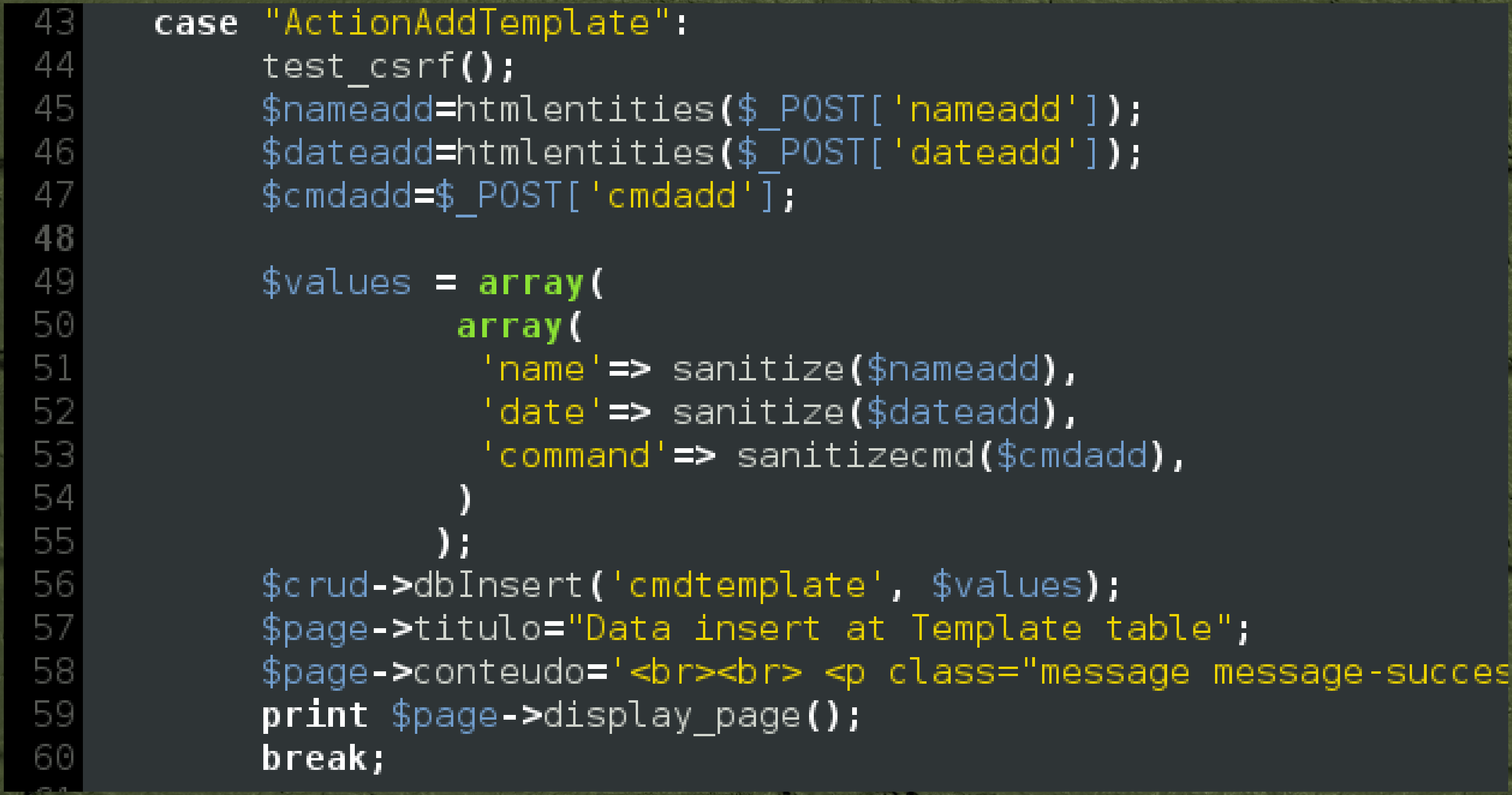


```
case "AddTemplate":
      $form = new form();
      $token = NoCSRF::generate( 'csrf_token' );
      $values = array(
                ':hidden'=>'csrf_token:'.$token,
                'name:text'=>'nameadd:Tool name',
                'date:text'=>'dateadd:'.gmdate("Y-m-d h:i"),
              );
      $action="ControlTemplate.php?page=ActionAddTemplate";
      $la.=$form->StartForm($action);
      $la.=$form->SimpleForm($values);
      $la.=$form->TextForm("CMD: ","cmdadd","command of tool here: \n You can us
      $la.=$form->ExitForm("submit");
      $page->titulo="Add Template of tool";
      $page->conteudo=$la;
      print $page->display_page();
      break;
```

NOZES

Simple code

nozes/controller/ControlTemplate.php



```
    case "ActionAddTemplate":
        test_csrf();
        $nameadd=htmlentities($_POST['nameadd']);
        $dateadd=htmlentities($_POST['dateadd']);
        $cmdadd=$_POST['cmdadd'];

        $values = array(
                 array(
                  'name'=> sanitize($nameadd),
                  'date'=> sanitize($dateadd),
                  'command'=> sanitizecmd($cmdadd),
                 )
                );
        $crud->dbInsert('cmdtemplate', $values);
        $page->titulo="Data insert at Template table";
        $page->conteudo='<br><br> <p class="message message-succes
        print $page->display_page();
        break;
```

NOZES

Security details

* Uses bcrypt at passwords.

* Uses sha256 at anti-csrf tokens.

* Uses htmlentities() function to mitigate XSS attacks.

* All communications with DB uses query parameterization in PDO.
(helper/class.crud.php)

Security details

* If you have idea to improve the code, create issue at project...

* If you get a bug, create issue at project...

Install

* Read the file:

nozes/doc/how_too_install.txt

For future

* Add queues with RabbitMQ.

* Implement timeout based protection to brute force mitigation in auth.

* Implement option to load multiples targets by list.

*Function to remove all “finishing” tasks.

NOZES

https://github.com/CoolerVoid/

THANK YOU !

NOZES