권한 검사

티키 권한 검사 (Tiki Permission Check, TPC): 티키 설치가 실패할 경우 정보의 추가 소스.
2012 년 10월 이후, (본 페이지에 첨부된) 독립형으로 존재하며, 또한 Tiki10 에 기능으로서 포함됨.

1. 개요

티키 권한 검사란 무엇인가?

만약 티키 설치관리자와 tiki-check.php 가 실패한다면, 티키 권한 검사를 사용하여 웹서버가 요구로 하는 파일시스템 권한에 관한 추가 상세내역을 발견하여 제대로 작동하도록 설정되도록 사용될 수 있습니다. 티키 권한 검사에 대한 권한은 수동적으로 고정될 수 있거나 (FPT 혹은 SSH 를 통하거나 다른 쉘 접근방식을 통하여 작은 갯수의 파일 전송 필요) 혹은 포함된 스크립트를 통할 수 있습니다. 티키 권한 검사는 티키를 웹서버 상에서 실행히기 위하여 어떤 파일 시스템 권한이 필요한지를 알아내기 위하여 사용될 수 있습니다. 이 권한 설정은 독특할 필요가 없습니다, 그렇기 때문에 귀하는 귀하게서 원하시거나 필요에 희아혀 보안 등급에 의존하여 제한을 더 두거나 덜 두도록 선택할 수 있습니다.

티키 권한 검사는 티키 자신으로부터 독립적인 파일 권한 문제들을 알아내는데 사용될 수 있습니다. 이러한 경우, 파일 권한은 수동적으로 조절되거나 다른 프로젝트에 적절한 어떠한 방식을 통하여 조절되어야만 합니다.

티키를 설치하는데 정보를 사용하기에 가장 편리한 방식은 setup.sh 수정을 통하는 것입니다. (곧 출시 예정)

사전 정의된 권한 모델

다양한 웹서버 설정 및 사례로 인하여, TPC는 다양한 사전 정의된 모델들을 제공하여 설치가 그들과 작동할지 여부를 확인하도록 합니다. 올바른 모델(들)이 알려지게되면, 적절한 명령어와 함께 설치 슬립트를 실행하는데 사용될 수 있습니다. 내장 권한 모델 (2012-11-11 부터 효력있음)

- insane
- mixed
- morepain
- moreowrry
- pain
- paranoia
- paranoia-suphp
- risky
- sbox
- worry

쉘 접근 없다면, 권한은 FTP 혹은 다른 방식에 의하여 설정되어야 합니다. 이는 많은 작업이 될 수도 있습니다, 그 이유는 어떤 파일과 서브디렉토리들이 쓰기가능해야하지만, 쓰기가능할 필요가 없는 것들은 쓰기 권한이 주어지면 안되기 때문입니다. 이상적이라면, 이러한 설치들 (예: 공유 호스팅)이 SuPHP 웹서버 보호를 사용하여 권한을 유용한 단계까지 (비록 이론적 최적상태가 아닐지라도) 설정하는 것이 손쉽게 되는 것입니다.

어디에서 구할 수 있나?

티키 권한 검사는 트렁크에 제공되며 독립형으로 다운로드 될 수 있습니다. Tiki10 내부에도 제공됩니다 (2012-10-22 이후부터). 독립형 버전은 티키의 그 어떠한 버전과도 작동을 할 것입니다 (현재 예측은 작동을 해야한다고 보고 있습니다) 본 페이지의 하단에, 알파 버전이 첨부되어 있습니다.

가장 최신 버전의 코드는 다음 위치에 있습니다:

- https://svn.code.sf.net/p/tikiwiki/code/trunk/permissioncheck/
- https://svn.code.sf.net/p/tikiwiki/code/branches/11.x/permissioncheck/]
- https://svn.code.sf.net/p/tikiwiki/code/branches/10.x/permissioncheck/]

2. 티키 권한 검사 활성화 및 비활성화 하기

중요한 문제는 티키 권한 검사를 활성하 및 비활성화 하는 것입니다. 필요한 정보를 취득했으면, 비활성화하는 것을 강력 추천합니다, 이는 몇몇 하위디렉터리들이 테스트 목적으로 전역 쓰기 가능하게 설정되며 파일들의 소유권 ((*user*/*group*) 이 대중에게 노출되기 때문입니다 (하지만, 웹서버의 설정에 따라, 가능하다면 htaccess 보호를 사용할 수도 있으실 것입니다).

2.1. 티키 권한 검사를 쉘에서 이용

sh (혹은 *bash*, *dash*) 와 같은 쉘을 사용하여 티키 문서 루트에 있는 `prepare_permissioncheck.sh` 스크립트를 실행하십시오.

2.1.1. 스크립트 권한 설정

티키의 문서 루트에 있음:
`chmod 600 prepare_permissioncheck.sh`

2.1.2. htaccess 권한 설정

티키의 문서 루트에 있음:
`chmod 644 permissioncheck/.htaccess`
만약 **.htaccess** 이 존재하지만 웹서버에서 읽을 수 없다면, 문제가 발생할 수도 있습니다.

이는 티키 권한 검사가 쉘 스크립트에 의하여 활성화 혹은 비활성화 될 때마다 진행됩니다. 그러므로 대부분의 경우, 수동으로 진행할 필요가 없습니다.

2.1.3. 쉘을 통하여 활성화

티키의 문서 루트에 있음:
`sh prepare_permissioncheck.sh enable`

2.1.4. 쉘을 통하여 비활성화

티키의 문서 루트에 있음:
`sh prepare_permissioncheck.sh disable`

2.2. 티키 권한 검사를 FTP 를 통하여 사용

쉘 접근이 없이 권한을 설정하는 것은 쉬운 것이 아닙니다. 지역 파일 권한을 설정하고 업로드를 하거나 FTP를 통하여 파일을 설정할 수 있습니다 (두 경우 모두: **enable/disable**). 추가로 티키 권한 검사를 **활성화** 하려면 `permissioncheck/yes.bin` 를 `permissioncheck/permission_granted.bin` 로 복사하고 **비활성** 하려면 `permissioncheck/no.bin` 를 `permissioncheck/permission_granted.bin` 로 복사하여야 합니다. (두 경우 모두: 그 후 FTP 로 다음을 업로드 합니다 `permissioncheck/permission_granted.bin`).

2.2.1. FTP chmod 를 통한 일반 설정

```
chmod 755 permissioncheck
chmod 644 permissioncheck/check.php
chmod 644 permissioncheck/functions.php.inc
chmod 600 permissioncheck/_htaccess
chmod 644 permissioncheck/.htaccess if it exists
chmod 600 permissioncheck/.htpasswd
chmod 644 permissioncheck/index.php
chmod 444 permissioncheck/no.bin
chmod 444 permissioncheck/permission_print.php.inc
chmod 644 permissioncheck/permission_granted.bin
chmod 644 permissioncheck/permission_granted.php.inc
chmod 644 permissioncheck/usecases.php.inc
chmod 644 permissioncheck/usecases.txt
chmod 444 permissioncheck/yes.bin
```

htaccess 권한 설정
만약 티키 권한 검사가 *permissioncheck/* 내부의 기존의 **.htaccess** 에 의하여 보호된다면, 티키 문서 루트에 다음을 확인하십시오:
`chmod 644 permissioncheck/.htaccess`
만약 **.htaccess** 가 존재하지만 웹서버에서 읽어들일 수 없다면, 문제가 발생할 수도 있습니다.

2.2.2. via FTP chmod 를 통하여 활성화

`permissioncheck/new_htaccess` 를 (임의의 내용으로) 생성, `permissioncheck/yes.bin` 를 `permissioncheck/permission_granted.bin` 에 복사하고 둘 다 업로드, 다음과 같이 FTP 서버에서 파일 권한 변경:

```
chmod 644 permissioncheck/create_new_htaccess.php
chmod 777 permissioncheck/insane
chmod 777 permissioncheck/insane/check.php
chmod 700 permissioncheck/mixed
chmod 660 permissioncheck/mixed/check.php
chmod 705 permissioncheck/morepain
chmod 606 permissioncheck/morepain/check.php
chmod 705 permissioncheck/moreworry
chmod 604 permissioncheck/moreworry/check.php
chmod 666 permissioncheck/new_htaccess
chmod 701 permissioncheck/pain
chmod 606 permissioncheck/pain/check.php
chmod 770 permissioncheck/paranoia
chmod 600 permissioncheck/paranoia/check.php
chmod 701 permissioncheck/paranoia-suphp
chmod 600 permissioncheck/paranoia-suphp/check.php
chmod 775 permissioncheck/risky
chmod 664 permissioncheck/risky/check.php
chmod 701 permissioncheck/worry
chmod 604 permissioncheck/worry/check.php
```

2.2.3. FTP chmod 를 통하여 비활성화

`permissioncheck/no.bin` 를 `permissioncheck/permission_granted.bin` 로 복사하고 업로드, FTP 서버에서 다음과 같이 권한 설정 변경:

```
chmod 000 permissioncheck/create_new_htaccess.php
chmod 700 permissioncheck/insane
chmod 600 permissioncheck/insane/check.php
chmod 700 permissioncheck/mixed
chmod 600 permissioncheck/mixed/check.php
chmod 700 permissioncheck/morepain
chmod 600 permissioncheck/morepain/check.php
chmod 700 permissioncheck/moreworry
chmod 600 permissioncheck/moreworry/check.php
chmod 600 permissioncheck/new_htaccess
chmod 700 permissioncheck/pain
chmod 600 permissioncheck/pain/check.php
chmod 700 permissioncheck/paranoia
chmod 600 permissioncheck/paranoia/check.php
chmod 700 permissioncheck/paranoia-suphp
chmod 600 permissioncheck/paranoia-suphp/check.php
chmod 700 permissioncheck/risky
chmod 600 permissioncheck/risky/check.php
chmod 700 permissioncheck/worry
chmod 600 permissioncheck/worry/check.php
```

3. 권한 개요: 예제

http://example.org/permissioncheck/
http://demo.tiki.org/pd/permissioncheck/
http://demo.tiki.org/10x/permissioncheck/
http://demo.tiki.org/trunk/permissioncheck/

3.1. 티키 권한 검사 사용하기

자신의 티키 설치 경로 /permissioncheck/ 를 방문하면 TPC 메인 페이지를 보게 될 것입니다. 위의 예제에서 example.com 도메인을 귀하의 도메인으로 교체하십시오. 페이지가 이것은 비활성화 되어있습니다 라고 말하면, 활성화를 해주셔야 합니다. 이러한 권한들에 대하여 모든 권한 모델, 사용자, 그룹 및 파일 권한 이 보여야 하며, 이 모델이 작동을 할 것인지 여부에 대한 힌트도 보여야 합니다. 작동을 할 것 같은 모델명을 기록해두십시오. 후에 필요하게 될 것입니다

4. 티키 권한 검사로부터의 정보 사용하기

4.1. 쉘 접근

티키 루트 디렉터리로 가서 설치 스크립트를 작동할 것처럼 보이는 모델명 중 하나와 함께 실행하십시오:
`sh setup.sh $model`↵
여기서 `$model` 를 위에 적어놓으신 것으로 교체하십시오. 이 모델이 여전히 작동하지 않는다면, 다른 것으로 시도하십시오. 작동하는 모델이 없다면, 하나씩 번갈아 가며 모든 사전 정의된 모델들을 시도해 보시고 결과를 지켜보십시오

5. setup.sh 의 명령어

5.1. 일반 명령어

- default
- menu
- nothing

5.2. 전통 명령어

- fix
- open

5.3. 사전정의된 모델들

- insane
- morepain
- moreworry
- pain
- paranoia
- paranoia-suphp
- risky
- sbox
- worry

5.4. 미세 조절 가능한 권한 부분들

5.4.1. 전체 티키 트리

- gmr
- gmw
- gmx
- gpr
- gpw
- gpx
- omr
- omw
- omx
- opr
- opw
- opx
- umr
- umw
- umx
- upr
- upw
- upx

5.4.2. 특수 디렉터리 (웹서버 쓰기 접근)

- sdgmw
- sdgpw
- sdomw
- sdopw
- sdumw
- sdup↵

6. 사용자 지정된 사용 케이스

경고: 초보자에게는 권장되지 않습니다

임의의 사용자 케이스가 추가될 수 있습니다. 이는 3단계를 통하여 빠르고 쉽게 이루어집니다:
1) 사용 케이스명을 정의하고 이 이름을 서브디렉터리 `permissioncheck/` 의 밑에 이 이름으로 디렉터리를 추가하고 `permissioncheck/check.php` 를 새 사용자 케이스 서브디렉터리로 복사하십시오.
2) 8진법의 서브디렉터리 읽기 (기본) 권한, 8진법의 서브디렉터리 쓰기 권한 및 8진법의 파일 쓰기 권한을 정의하십시오. A-+permissioncheck/usecases.bin+- 에 이름과 권한을 콜론으로 구분하여 추가하십시오. 줄 끝부분에서 조심하십시오, 애플 (CR) 과 윈도우 (CR+LF) 는 아직 시험하지 않았습니다.
3) 사용자 케이스를 티키의 주 디렉터리 내부의 `setup.sh` 에 추가하십시오. 주 프로그램 내부의 스크립트의 마지막 부분: copy the line `php) permission_via_php_check ;;` 줄을 복사하시고 (*새 줄에서 해야만 합니다*) 시작하는 `php)` 를 `name)` 으로 교체하십시오, 여기서 *name* 은 위의 1)에서 선택한 것입니다.

7. 관련 컨텐츠

- https://dev.tiki.org/Permission+Check
- 서버 검사
- htaccess
- https://dev.tiki.org/How+to+avoid+direct+access+of+a+file↵