Hiki

最近のHikiってどう？

かずひこ

NaCl (ネットワーク応用通信研究所)

もともとHikiって何？

Rubyで書かれたWikiクローン

- オリジナルWikiに似たシンプルな書式
- (一応) tDiary互換なテーマ機能
- プラグインによる機能拡張
- Amritaによる柔軟なテンプレート
- ページにカテゴリ付けできる
- Rubyで記述されている

使われているの？

- HikiWikisのページに109サイト載っている

使われているの？

- HikiWikisのページに109サイト載っている
- うちのwikifarm内だけで124サイト (3860ページ) もある

使われているの？

- HikiWikisのページに109サイト載っている
- うちのwikifarm内だけで124サイト (3860ページ) もある
- NaClでも採用されている

セキュリティホール発覚 (1)

- 管理認証をバイパスできる
  - セッション管理していなかったので、保存時のクエリーをいきなり送ることで設定を書き換えることができた
  - 管理モードに入ったた時にセッションを作り、設定の変更をする際にそのセッションを確認するように修正

セキュリティホール発覚 (1)

- 管理認証をバイパスできる
  - セッション管理していなかったので、保存時のクエリーをいきなり送ることで設定を書き換えることができた
  - 管理モードに入ったた時にセッションを作り、設定の変更をする際にそのセッションを確認するように修正

→ セッション管理重要

セキュリティホール発覚 (2)

- CGI 実行ユーザ権限で何でもできる
  - 管理モードから設定ファイルを書き出す際、エスケープ処理がされておらず、任意のrubyコードを送り込めた
  - この設定ファイルはHiki実行時にKernel#evalされる
  - さっきの脆弱性と組み合わせると...

```
conf_list.each do |c|
  f.puts( %Q|#{c} = "#{eval(c)}"| ) if c
end
```

セキュリティホール発覚 (2)

- CGI 実行ユーザ権限で何でもできる
  - 管理モードから設定ファイルを書き出す際、エスケープ処理がされておらず、任意のrubyコードを送り込めた
  - この設定ファイルはHiki実行時にKernel#evalされる
  - さっきの脆弱性と組み合わせると...

```
conf_list.each do |c|
  f.puts( %Q|#{c} = "#{eval(c)}"| ) if c
end
```

→ エスケープ重要

セキュリティホール発覚 (3)

- 修正が不十分だった orz
  - String#inspectは'#{.....}'をエスケープできません

```
conf_list.each do |c|
  f.puts( %Q|#{c} = "#{eval(c).inspect}"| ) if c
end
```

セキュリティホール発覚 (3)

- 修正が不十分だった orz
  - String#inspectは'#{.....}'をエスケープできません

```
conf_list.each do |c|
  f.puts( %Q|#{c} = "#{eval(c).inspect}"| ) if c
end
```

→ String#dump重要

→ というかKernel#eval禁止...

バグは続くよどこまでも

- たまにパスワードなしで管理モードに行ける
  - 設定ファイルのevalを$SAFE=4スレッドの中で行うように変更した時に、スレッドのjoinを忘れていた

```
Thread.start {
  $SAFE = 4
  eval( cgi_conf, binding, "(hiki.conf)", 1 )
}
```

バグは続くよどこまでも

- たまにパスワードなしで管理モードに行ける
  - 設定ファイルのevalを$SAFE=4スレッドの中で行うように変更した時に、スレッドのjoinを忘れていた

```
Thread.start {
  $SAFE = 4
  eval( cgi_conf, binding, "(hiki.conf)", 1 )
}
```

→ 後かたづけ重要

管理者がデスマーチ

- 日記のタイトルがかなりやばい
  - 2003-11-10 生きてます
  - 2004-04-07 Hiki0.6.3リリース
  - 2004-06-21 Hiki0.6.4リリース
  - 2004-06-28 Hiki0.6.5リリース
  - 2004-07-13 Hikiの脆弱性に関する報告
  - 2004-07-26 デスマプロジェクト
    - 「土日の終電も結構混んでるんですね。ははは…」
  - 2004-09-17 生きてます
    - 「子供と遊びたいんですよ。ええ。」

管理者がデスマーチ

- 日記のタイトルがかなりやばい
  - 2003-11-10 生きてます
  - 2004-04-07 Hiki0.6.3リリース
  - 2004-06-21 Hiki0.6.4リリース
  - 2004-06-28 Hiki0.6.5リリース
  - 2004-07-13 Hikiの脆弱性に関する報告
  - 2004-07-26 デスマプロジェクト
    - 「土日の終電も結構混んでるんですね。ははは…」
  - 2004-09-17 生きてます
    - 「子供と遊びたいんですよ。ええ。」

→ サステイナビリティ重要

鬼の居ぬ間に洗濯

- 各種プラグインの修正・追加
  - 幸い、バグ報告やパッチはいろいろいただいた

鬼の居ぬ間に洗濯

- 各種プラグインの修正・追加
  - 幸い、バグ報告やパッチはいろいろいただいた
- mod_ruby対応
  - 高速化命！ mod_rubyラヴ

鬼の居ぬ間に洗濯

- 各種プラグインの修正・追加
  - 幸い、バグ報告やパッチはいろいろいただいた
- mod_ruby対応
  - 高速化命! mod_rubyラヴ
- TrackBack対応
  - 「るびま!」で欲しかっただけ

鬼の居ぬ間に洗濯

- 各種プラグインの修正・追加
  - 幸い、バグ報告やパッチはいろいろいただいた
- mod_ruby対応
  - 高速化命! mod_rubyラヴ
- TrackBack対応
  - 「るびま!」で欲しかっただけ

→ 手が速いの重要

下剋上！

そしてついに、2004-10-03 Hikiのプロジェクト管理者に！


プロジェクト: Hiki

概要

HikiはRubyによるWikiエンジンです。Ruby用html/xhtmlテンプレートライブラリAmritaを使用しているため、出力するHTMLを柔軟にカスタマイズすることができます。

- Development Status: 3 - Alpha
- Environment: Web Environment
- License: GNU General Public License (GPL)
- Natural Language: Japanese
- Operating System: OS Independent
- Programming Language: Ruby
- Topic: Communications

登録日: 2003-02-16 20:58
活発さ: 0%

開発者情報

プロジェクト管理者
hitoshi
fdiary

開発メンバー
4 [メンバー一覧]

下剋上！

そしてついに、2004-10-03 Hikiのプロジェクト管理者に！


プロジェクト: Hiki
概要

HikiはRubyによるWikiエンジンです。Ruby用html/xhtmlテンプレートライブラリAmritaを使用しているため、出力するHTMLを柔軟にカスタマイズすることができます。

- Development Status: 3 - Alpha
- Environment: Web Environment
- License: GNU General Public License (GPL)
- Natural Language: Japanese
- Operating System: OS Independent
- Programming Language: Ruby
- Topic: Communications

登録日: 2003-02-16 20:58
活発さ: 0%

開発者情報

プロジェクト管理者
hitoshi
fdiary

開発メンバー
4 [メンバー一覧]

→ トラックナンバー重要

→ それはそれとしてツッコミどころ満載...

Hikiが目指すもの

- 軟派なWiki
  - インストール簡単
  - プラグインでいろいろできる
    - ファイル添付とか
    - 履歴管理とか
  - 新規作成も日本語ページ名もブラケットネームもOK
  - WikiFarmも作れる
  - けっこう速い (mod_rubyを使えば)

Hikiが目指すもの

- 軟派なWiki
  - インストール簡単
  - プラグインでいろいろできる
    - ファイル添付とか
    - 履歴管理とか
  - 新規作成も日本語ページ名もブラケットネームもOK
    - WikiFarmも作れる
    - けっこう速い (mod_rubyを使えば)

→ 軟派上等

自分は硬派であります！

- BitChannelとか…

自分は硬派であります！

- BitChannelとか…
- ていうかp*****使えば？

流行るRubyプロジェクトの秘訣

- Rubyistにウケる
  - 勝手に開発が進む
- 非Rubyistにウケる
  - 勝手にニーズやアイデアが出てくる

流行るRubyプロジェクトの秘訣

- Rubyistにウケる
  - 勝手に開発が進む
- 非Rubyistにウケる
  - 勝手にニーズやアイデアが出てくる

→ 硬派なコード重要

→ 軟派なコンセプト重要

ToDo

- プラグインの設定画面をブラウザに出すようにする
- Hikiごとにプラグイン選択できるようにする
- 高速化のためにキャッシュ化
- 高速化のためにテンプレート変更？

ToDo

- プラグインの設定画面をブラウザに出すようにする
- Hikiごとにプラグイン選択できるようにする
- 高速化のためにキャッシュ化
- 高速化のためにテンプレート変更？

→ そんなことより、老舗旅館コードになる前にオーバーホール重要

いろいろ募集

- 開発する人
- インストールする人
- 使う人
- 使わせる人

いろいろ募集

- 開発する人
- インストールする人
- 使う人
- 使わせる人

→ あなた重要!

おしまい

ご静聴ありがとうございました

ご意見、ご質問など、なんでもどうぞ