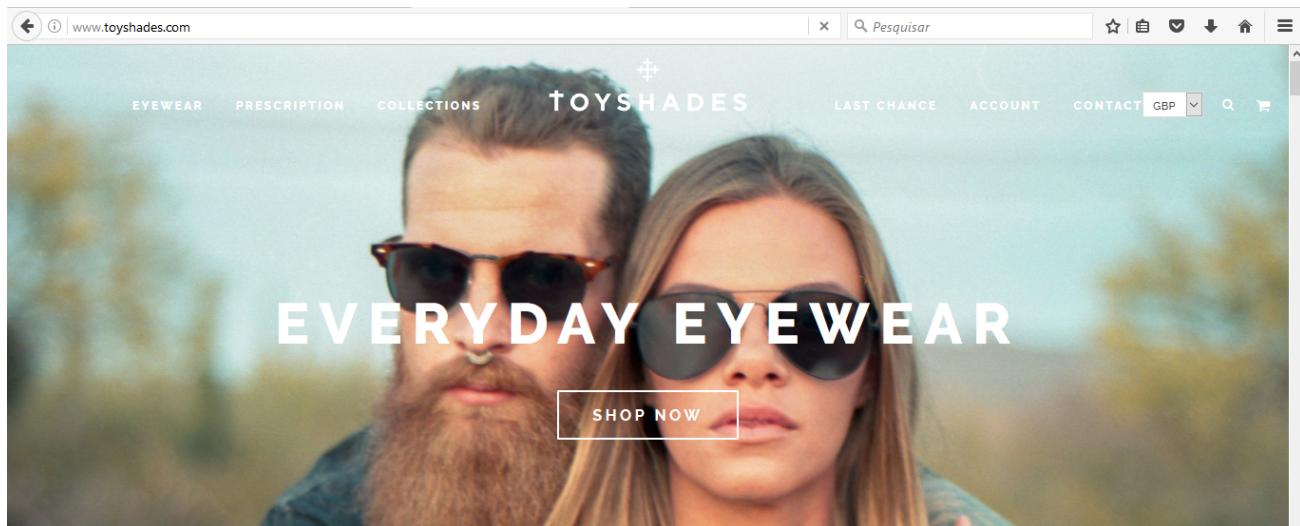


01

Falhas de segurança

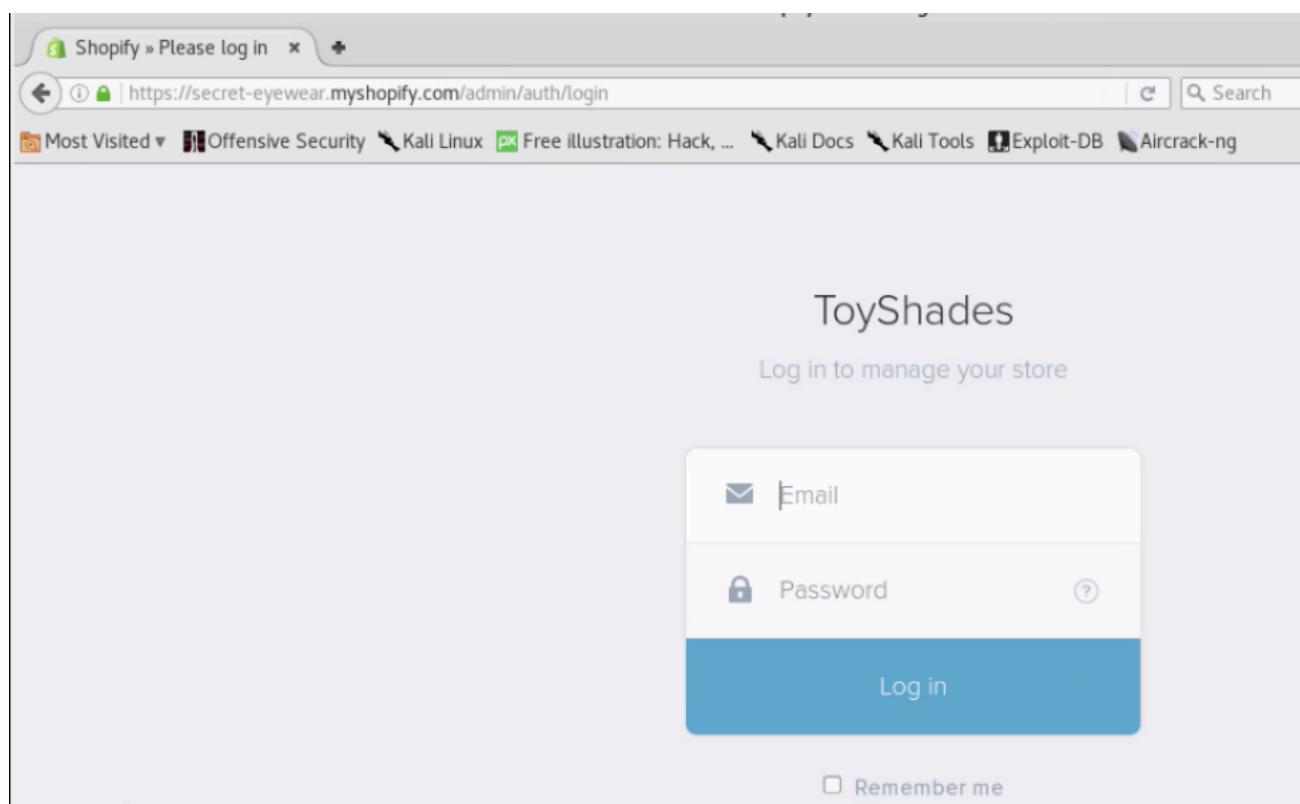
Transcrição

Nesta aula, vamos analisar outros tipos de ataques que podem ser realizados em ambientes da web. Vamos utilizar como exemplo uma loja virtual que faz uso da plataforma do *Shopify*. Primeiro, observamos o seguinte site:



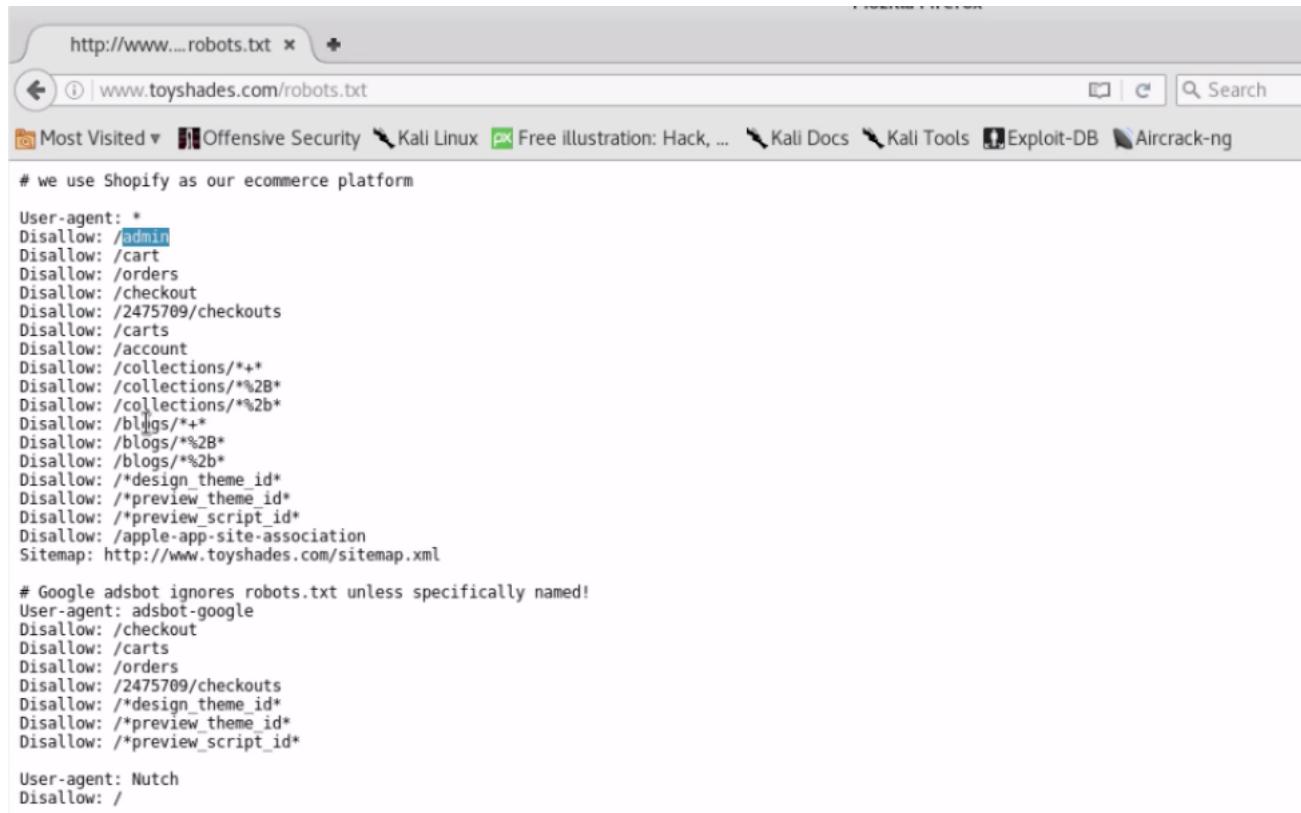
Este link corresponde a uma loja especializada em vender óculos. Para que o usuário acesse produtos e seus respectivos preços é preciso existir alguém que disponibilize e arrume essas informações para nós.

Um usuário mal intencionado pode tentar acessar a parte do site onde as informações são inseridas, isto é, uma página administrativa. Junto a URL principal, a www.toyshades.com/, podemos inserir palavras que normalmente são utilizadas para indicar links administrativos. Por exemplo, depois da barra acrescentamos: `administrador`, `administrator` e `adm`. Apenas a última alternativa funciona e acessando a www.toyshades.com/admin temos o seguinte:



Para acessar essa parte administrativa é preciso um usuário e senha cadastrados e assim o sistema verifica permissão de acesso da página. Se não houver checagem qualquer pessoa pode entrar na parte administrativa e fazer o que quiser com ela. Como desenvolvedores podemos escolher esconder algumas páginas dos mecanismos de busca.

Por questões estratégicas da empresa podemos escolher, por exemplo, que a página do `admin` não seja indexada. Para fazer isso utilizamos o `robots.txt`. Quando digitamos na URL `www.toyshades.com/robots.txt` temos o seguinte:



```

http://www....robots.txt x + 

http://www.toyshades.com/robots.txt

# we use Shopify as our ecommerce platform

User-agent: *
Disallow: /admin
Disallow: /cart
Disallow: /orders
Disallow: /checkout
Disallow: /2475709/checkouts
Disallow: /carts
Disallow: /account
Disallow: /collections/*+
Disallow: /collections/*%2B*
Disallow: /collections/*%2B*
Disallow: /blogs/*+
Disallow: /blogs/*%2B*
Disallow: /blogs/*%2B*
Disallow: /*design_theme_id*
Disallow: /*preview_theme_id*
Disallow: /*preview_script_id*
Disallow: /apple-app-site-association
Sitemap: http://www.toyshades.com/sitemap.xml

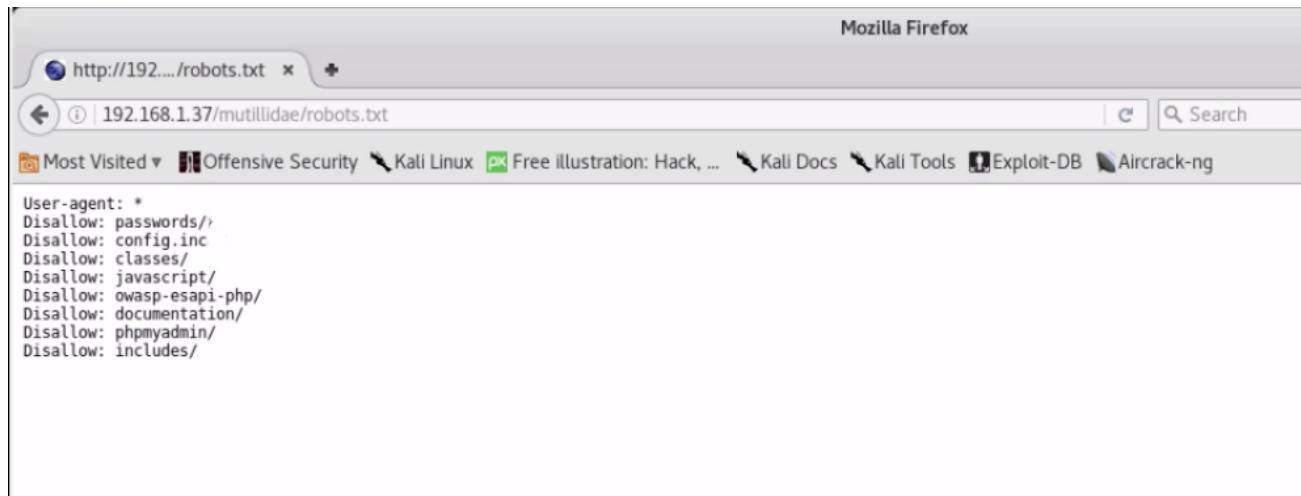
# Google adsbot ignores robots.txt unless specifically named!
User-agent: adsbot-google
Disallow: /checkout
Disallow: /carts
Disallow: /orders
Disallow: /2475709/checkouts
Disallow: /*design_theme_id*
Disallow: /*preview_theme_id*
Disallow: /*preview_script_id*

User-agent: Nutch
Disallow: /

```

Esta lista mostra endereços não indexados. O problema disso é que algumas destas páginas não possuem sistemas de autenticação tornando-as alvos de possíveis invasões. Portanto, como estratégia de segurança é preciso que páginas restritas sempre possuam sistemas de autenticação.

Agora, vamos acessar o site da *Multillidae* e verificar se existem páginas a ela vinculadas, as quais os desenvolvedores não indexaram na busca. Para observar isso podemos digitar no navegador `192.168.1.37/multillidae/robots.txt` e teremos :



```

Mozilla Firefox

http://192..../robots.txt x + 

http://192.168.1.37/multillidae/robots.txt

# Most Visited v Offense Security Kali Linux Free illustration: Hack, ... Kali Docs Kali Tools Exploit-DB Aircrack-ng

User-agent: *
Disallow: /passwords/
Disallow: /config.inc
Disallow: /classes/
Disallow: /javascript/
Disallow: /owasp-esapi-php/
Disallow: /documentation/
Disallow: /phpmyadmin/
Disallow: /includes/

```

O primeiro item que aparece na lista é o `/passwords` que significa, literalmente, senhas. É provável que o usuário não tenha acesso a essa parte do site e que o desenvolvedor tenha inserido nela algum tipo de verificação. Mas, será que o

desenvolvedor realmente adotou essa precaução? Para verificar isso podemos tentar acessar o seguinte:

192.168.1.37/mutillidae/passwords

Abrirá a seguinte página:

Name	Last modified	Size	Description
Parent Directory			
accounts.txt	17-Nov-2016 10:41	957	

Ou seja, o desenvolvedor não se precaveu, pois temos acesso as senhas. Ele pensou que não seria necessário inserir uma autenticação nesse trecho do site. Ainda, clicando no `accounts.txt`, temos acesso a diversos dados privados dos clientes:

Index	Name	Password	Role
1	admin	admin,g0t r00t?	Admin
2	adrian	somepassword	Zombie Films Rock!
3	john	monkey	I like the smell of confunk
4	jeremy	password	d1373 1337 speak
5	bryce	password	I Love SANS
6	samurai	samurai	Carving fools
7	jim	password	Rome is burning
8	bobby	password	Hank is my dad
9	simba	password	I am a super-cat
10	dreveil	password	Preparation H
11	scotty	password	Scotty do
12	cal	password	C-A-T-S Cats Cats Cats
13	john	password	Do the Duggie!
14	kevin	42	Doug Adams rocks
15	dave	set	Bet on S.E.T. FTW
16	patches	tortoise	meow
17	rocky	stripes	treats?
18	tim	lanmaster53	Because reconnaissance is hard to spell
19	ABaker	SoSecret	Muffin tops only
20	PPan	NotTelling	Where is Tinker?
21	CHook	JollyRoger	Gator-hater
22	james	i<3devs	Occupation: Researcher
23	user	user	User Account
24	ed	pentest	Commandline KungFu anyone?

Existe uma ferramenta que nos auxilia neste tipo de mapeamento, a **nikto**. Ela é utilizada para verificar o `host`, portanto, no Terminal, vamos escrever `nikto -h` e inserimos a URL da página sobre a qual desejamos fazer uma busca:

```
> nikto -h "http://192.168.1.37/mutillidae/"
```

Dando um "Enter" nisso a `nikto` começa a realizar um mapeamento e assim que é finalizado temos todas as páginas encontradas pela ferramenta:

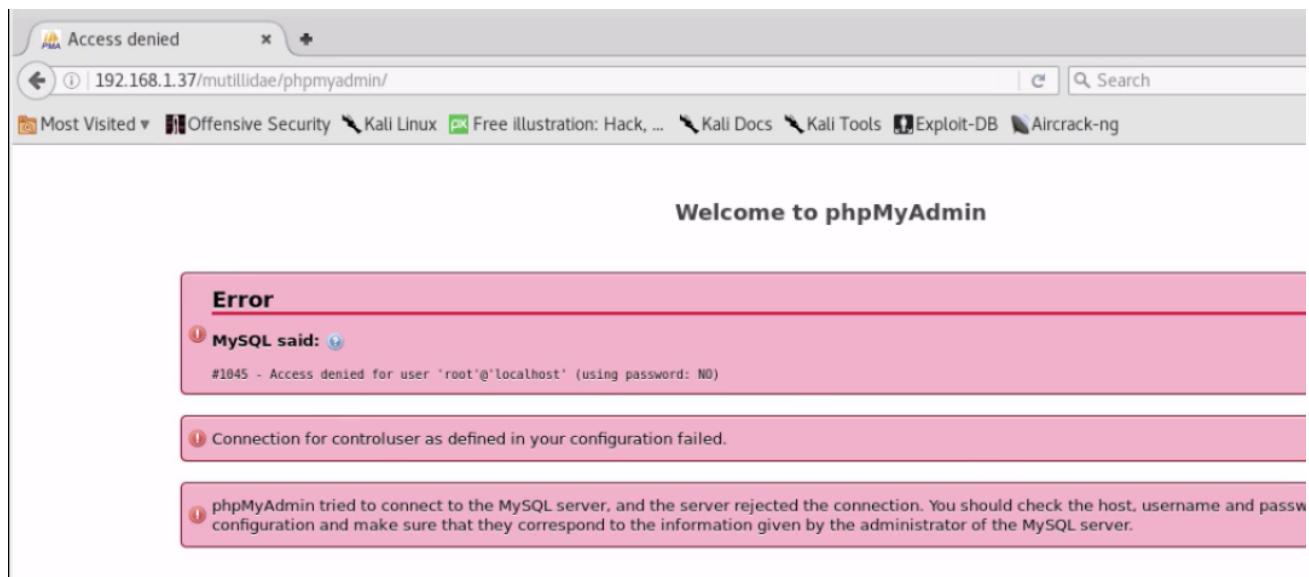
```

root@kali: ~
File Edit View Search Terminal Help
+ OSVDB-5292: /mutillidae/index.php?themesdir=http://cirt.net/rfiinc.txt?: RFI from RSnake's
  rfi-locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /mutillidae/index.php?this_path=http://cirt.net/rfiinc.txt??: RFI from RSnake's
  rfi-locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /mutillidae/index.php?txt=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (l
  -locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /mutillidae/index.php?up=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (h
  locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /mutillidae/index.php?url=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (l
  -locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /mutillidae/index.php?w=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (ht
  ocations.dat) or from http://osvdb.org/
+ OSVDB-5292: /mutillidae/index.php?way=http://cirt.net/rfiinc.txt?????????????????: RFI from R
  .org/weird/rfi-locations.dat) or from http://osvdb.org/
+ /mutillidae/phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /mutillidae/.git/index: Git Index file may contain directory listing information
+ /mutillidae/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ OSVDB-3092: /mutillidae/phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL data
  ed or limited to authorized hosts.
+ OSVDB-3268: /mutillidae/webservices/: Directory indexing found.
+ /mutillidae/webservices/: Webservices found
+ /mutillidae/.git/config: Git config file found. Infos about repo details may be present.
+ 7545 requests: 0 error(s) and 186 item(s) reported on remote host
+ End Time: 2016-11-18 10:26:59 (GMT-5) (53 seconds)

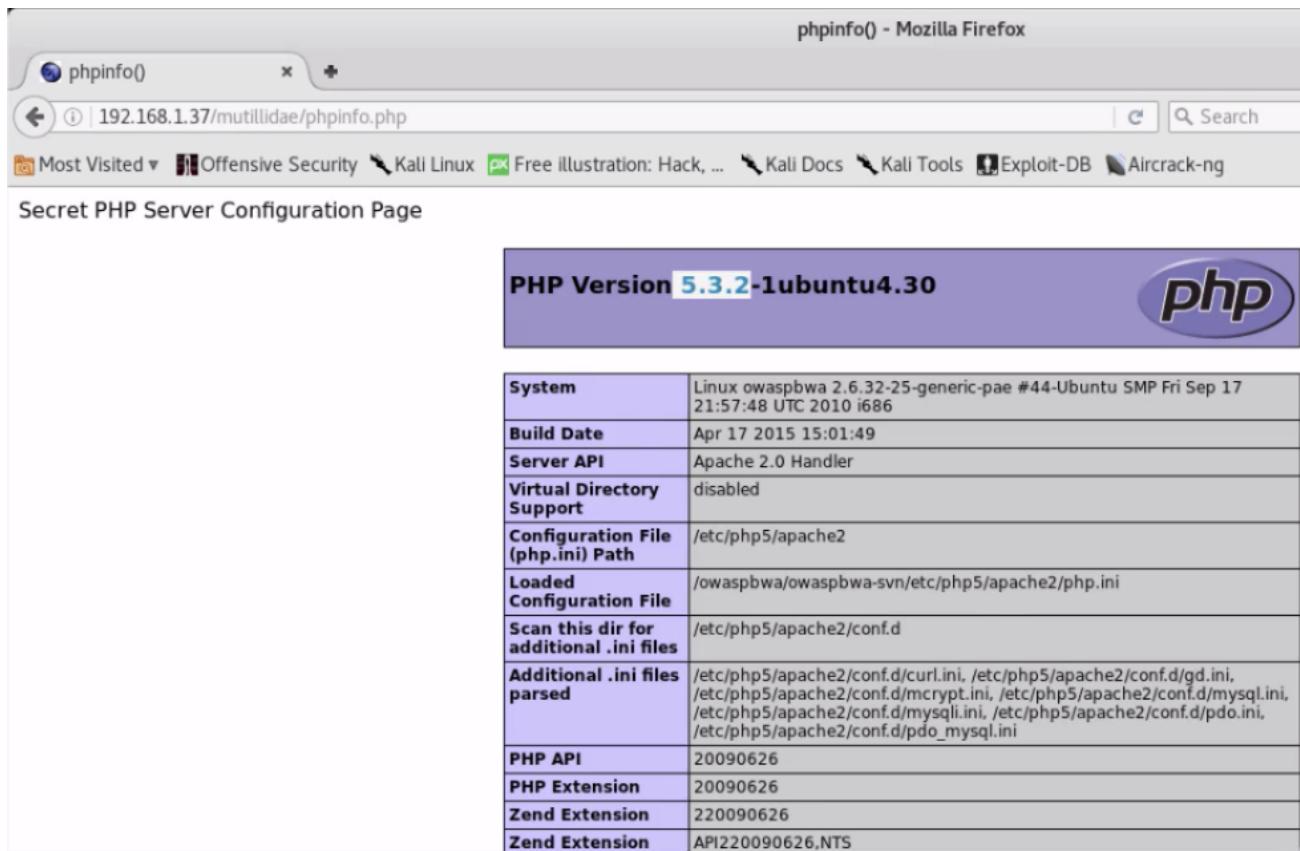
```

Uma das páginas mapeada chama atenção, a `/mutillidae/phpmyadmin/`. Ao lado dela aparece um pequeno resumo sobre o link, trata-se de uma página administrativa voltada para o Banco de dados do MySQL. Teoricamente, devido a sua importância, essa página não deve estar disponível para acesso de qualquer pessoa. Vamos testar!

Ao digitarmos no navegador `192.169.1.37/mutillidae/phpmyadmin`, veremos o seguinte resultado:



O acesso é de fato negado, portanto, o desenvolvedor realmente se precaveu. Mas, ao acessarmos o `192.169.1.37/mutillidae/phpinfo.php` conseguimos entrar na página:



PHP Version 5.3.2-1ubuntu4.30	
System	Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686
Build Date	Apr 17 2015 15:01:49
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/owaspbwa/owaspbwa-svn/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/curl.ini, /etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension API	API220090626.NTS

Neste outro link temos acesso a diversas informações relevantes, pois, o desenvolvedor acabou não se dando ao trabalho de esconder o que está aí descrito. Essas informações, por exemplo, a **Apache Version** são o suficiente para um futuro ataque!