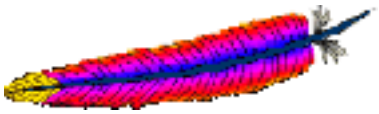
Apache - отключение вывода системной информации

Опубликовано muff в Чт, 2011-12-29 15:01



Если кто-то сталкивался с теорией взлома, то ему известно, что злоумышленник первым делом пытается определить версию операционной системы и установленного ПО, чтобы воспользоваться доступными уязвимостями. Посмотрим, какую информацию выдает web-сервер Apache.

Подключимся к веб-серверу и после отправки запроса (запрос HEAD / HTTP/1.0; ну и не забываем о необходимости нажать "Enter") посмотрим, какую информацию можно почерпнуть из заголовков сервера:

```
# telnet localhost 80
 Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

  HTTP/1.1 200 OK
Date: Thu, 29 Dec 2011 12:03:13 GMT
Server: Apache/2.2.17 (FreeBSD) DAV/2 PHP/5.2.17 with Suhosin-Patch mod_ssl/2.2.17
OpenSSL/0.9.8e mod_perl/2.0.5 Perl/v5.8.9
 X-Powered-By: PHP/5.2.17
 Set-Cookie: SESSd41d8cd98f00b204e9800998ecf8427e=va2u6rhi4c46p2r281ce56f860;
expires=Sat, 21-Jan-2012 15:36:33 GMT; path=/
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Thu, 29 Dec 2011 12:03:13 GMT
Cache-Control: store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8

Connection closed by foreign host.
```

Из ключевых моментов стоит отметить, что **Apache** раскрывает свою версию, установленную операционную систему и версию **PHP**. А это уже немало.

Для управления вывода этой информации используются директивы **ServerTokens** и **ServerSignature**.

ServerTokens

Синтаксис: *ServerTokens Major|Minor|Min[imal]|Prod[uctOnly]|OS|Full*

Примеры выводимых заголовков:

ServerTokens Prod[uctOnly]
Server sends (e.g.): *Server: Apache*

ServerTokens Major
Server sends (e.g.): *Server: Apache/2*

ServerTokens Minor
Server sends (e.g.): *Server: Apache/2.0*

ServerTokens Min[imal]
Server sends (e.g.): *Server: Apache/2.0.41*

ServerTokens OS
Server sends (e.g.): *Server: Apache/2.0.41 (Unix)*

ServerTokens Full (or not specified)
Server sends (e.g.): *Server: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2*

ServerSignature

Syntax: *ServerSignature On|Off|EMail*

Добавим в конфигурационный файл **Apache** такие строки:

```
ServerTokens ProductOnly
ServerSignature Off
```

Дадим команду на перезапуск сервера **Apache**:

```
# apachectl graceful
```

Проверим, какие заголовки теперь выводятся:

```
# telnet localhost 80
 Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 29 Dec 2011 12:07:10 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Set-Cookie: SESSd41d8cd98f00b204e9800998ecf8427e=c2to8i5ude7u6l7qe49946o192;
expires=Sat, 21-Jan-2012 15:40:30 GMT; path=/
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Thu, 29 Dec 2011 12:07:10 GMT
Cache-Control: store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8

Connection closed by foreign host.
```

Осталось еще "спрятать" версию **PHP**. Чтобы отключить в **PHP** передачу служебной информации в заголовки веб-сервера, необходимо в **php.ini** установить значение переменной **expose_php** в значение **Off**:

```
# cat /usr/local/etc/php.ini | grep expose_php
 expose_php = Off
```

Изменения вступят в силу после перезапуска веб-вервера.

```
# apachectl graceful
```

Проверяем результат:

```
# telnet localhost 80
 Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 29 Dec 2011 12:10:18 GMT
Server: Apache
Set-Cookie: SESSd41d8cd98f00b204e9800998ecf8427e=iscdhol2rk8cd7huoqpbsepnf6;
expires=Sat, 21-Jan-2012 15:43:38 GMT; path=/
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Thu, 29 Dec 2011 12:10:18 GMT
Cache-Control: store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8

Connection closed by foreign host.
```

Кажется достигли цели... Версии ПО скрыты от посторонних.

Источник (получено *2026-05-09 19:59*):
http://muff.kiev.ua/content/apache-otklyuchenie-vyvoda-sistemnoi-informatsii