



# **Základná ochrana pred útokmi na web I**

---

**Odporúčanie VJ CSIRT  
08.04.2024**



## 1. Neoprávnené vykonávanie príkazov

Pod neoprávneným vykonávaním príkazov rozumieme zneužitie systému na vykonanie príkazu, ktorý nebol mienený na vykonanie v prvom rade. Ako príklad uvedieme možnosť vykonať príkaz ping, pre ktorý stačí zadať IP adresu cieľa.

```
Ping for FREE
Enter an IP address below:
127.0.0.1 submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_req=3 ttl=64 time=0.036 ms
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.036/0.048/0.063/0.013 ms
```

Vďaka nedostatočnej implementácii je ale možné zneužiť mechanizmus, ktorým sa služba na serveri spúšťa.

Útočník dokáže využiť funkciu príkazového riadku na zreťazenie príkazov, a teda vykonať viacero príkazov súčasne. Útočník takto dokáže vykonávať akékoľvek príkazy s právami používateľa, ktorý spustil web server. Môžeme použiť operátor „;“, „&&“ alebo „|“ na zreťazenie príkazov a vytvoriť tak napríklad príkaz „**127.0.0.1 ; cat /etc/passwd**“, kde sa najprv vykoná prvá legitímna časť a následne kód útočníka, ktorý zobrazí obsah súboru /etc/passwd. Na obrazovku sa vypíše celkový výstup procesu.

Bez ošetrenia takejto zraniteľnosti otvárame veľmi vážnu dieru do systému, kde aj útočník na veľmi nízkej technickej úrovni dokáže spôsobiť rozsiahle škody.

## Ping for FREE

Enter an IP address below.

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_req=3 ttl=64 time=0.064 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.019/0.049/0.065/0.022 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:103:106::/var/run/dbus:/bin/false
whoopsie:x:104:107::/nonexistent:/bin/false
landscape:x:105:110::/var/lib/landscape:/bin/false
sshd:x:106:65534::/var/run/sshd:/usr/sbin/nologin
test:x:1000:1000:test,,,:/home/test:/bin/bash
```

### 1.1. Ochrana

Ochrana pred takýmto typom útoku spočíva v zablokovaní vkladania iných reťazcov ako tých, ktoré sú očakávaným vstupom. V našom prípade funkcie PING očakávame vstup vo formáte IP adresy **X.X.X.X**, kde X musia byť čísla o max. veľkosti jedného bajtu. Číslo spracúvame po jednotlivých zložkách adresy, a teda sa nám nikdy nevykoná prípadný vložený kód. Čím detailnejšie nastavíme obmedzenia, tým vyšší stupeň ochrany dosiahneme.

## 2. Zraniteľnosť v ceste k súboru

Zraniteľnosť v ceste k súboru spočíva vo vybočení z predpokladaných stránok, ktoré mali byť zobrazené a miesto nich sú načítané systémové súbory, prípadne škodlivé súbory z iných lokalít na internete.

V našom príklade je stránka page.php určená ako zobrazovač obsahu ktorý mu posunul iný skript na webe. Kvôli zlej implementácii je možné podsunúť reťazec, ktorý vypíše obsah súboru so zoznamom používateľov systému, prípadne je možné vložiť stránku z iného zdroja, napríklad [www.evilsite.com/evil.php](http://www.evilsite.com/evil.php). Takto je možné, aby sa vykonal cudzí kód na zraniteľnom systéme.

Po navštívení nasledovnej adresy:

```
127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../../../../../../../../../../../etc/passwd
```

sme dostali odpoveď obsahujúcu zoznam používateľov a ich skupín v hornej časti stránky.



Približná časť vyzerá nasledovne:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/shadowx:4294967295:root:/root:/bin/sh games:x:60:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh list:x:38:38:www-list:/var/www:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats:/usr/libuid:x:100:101:/:/var/lib/libuid:/bin/sh syslog:x:101:103:/:/home/syslog:/bin/false whoopsie:x:104:107:/:/nonexistent:/bin/false landscape:x:105:110:/:/home/landscape:/bin/false test:x:1000:1000:test:/:/home/test:/bin/bash
```

### 2.1. Ochrana

Ochrana pred týmto útokom spočíva v programátorskom ošetrení skriptu, ktorý vykonáva načítavanie iných stránok. Jedným z opatrení je obmedziť vstup akéhokoľvek iného reťazca znakov, ako sú povolené názvy súborov, ktoré má používateľ právo spustiť. Ďalšou ochranou je uzamknutie webserveru (Apache) v umelom koreňovom adresári (chroot).

### 3. SQL injection

SQL injection bol a stále je jeden z najpopulárnejších útočných vektorov, kde vďaka neošetrenému vstupu do databázy vie útočník vykonať SQL dotazy. Na základe výstupov z databázy dokáže útočník získať dáta zo systému (informácie o zákazníkoch, mená, heslá, čísla kreditných kariet, ...). V prípade niektorých konfigurácií databázového serveru útočník dokáže vykonávať systémové príkazy s oprávneniami SQL servera.

V našom príklade sme k požadovanému vstupu čísla používateľa, o ktorom chceme získať údaje, pridali aj SQL dopyt (`1' union select user_id, password from users where 'x' = 'x`), na základe ktorého sme vypísali obsah stĺpcov v tabuľke ku ktorým pôvodne nebolo možné pristupovať.

```
User ID:
1' union select user_id, passv Submit

ID: 1' UNION SELECT user_id,password FROM users WHERE 'x'='x
First name: admin
Surname: admin

ID: 1' UNION SELECT user_id,password FROM users WHERE 'x'='x
First name: 1
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user_id,password FROM users WHERE 'x'='x
First name: 2
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user_id,password FROM users WHERE 'x'='x
First name: 3
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user_id,password FROM users WHERE 'x'='x
First name: 4
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user_id,password FROM users WHERE 'x'='x
First name: 5
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

#### 3.1. Ochrana

Ochrana pred SQL injection spočíva v zabránení vloženia SQL kódu do spracúvaného poľa aplikácie. Najsilnejšiu ochranu ponúkajú takzvané predpripravené výrazy (prepared statements), ktoré obmedzujú vstup od používateľa. Je možné rozlíšiť jednotlivé parametre ktoré vstupujú do SQL reťazca a obmedziť ich (integer, string...) tak, aby nebolo možné zadávať čokoľvek iné.