



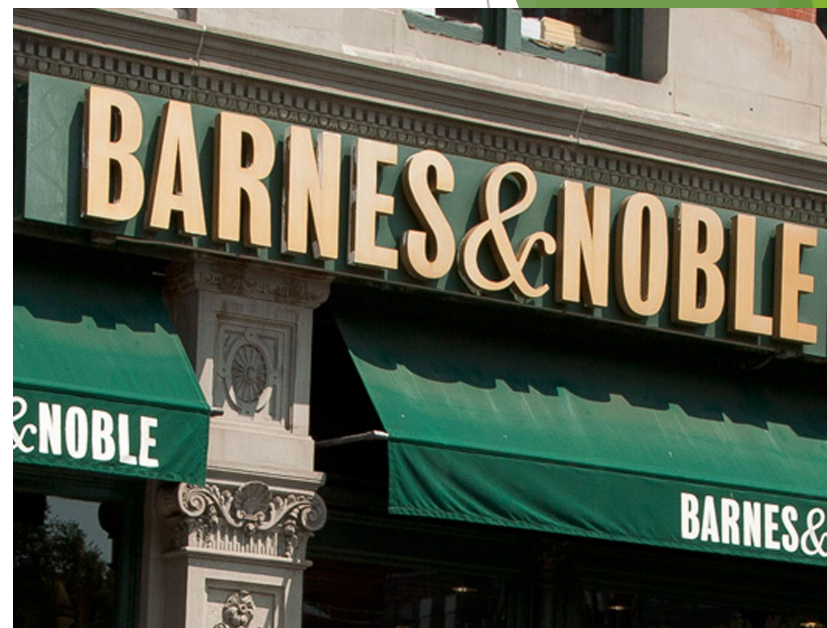
Burp Proxy Analysis for Barnes & Noble

MIS 5211: Introduction to Ethical Hacking

Mengqi He

Barnes & Noble

- ▶ Largest retail bookseller in the United States.
- ▶ 640 retail stores over the US.
- ▶ Products:
 - ▶ sells books, eBooks, magazines, toys & games, music, DVD and Blu-ray, and related products and services
- ▶ Started selling books online since the late 1980s.
- ▶ Security issue: credit card data breach
 - ▶ Victims: customers who shopped in August and September at 63 B&N stores across the country.
 - ▶ Hackers broke into the keypads in front of registers where customers swipe their credit cards and enter their PINs.



Proxy Intercepting result: Sign-in page

Subdomain of needle.com, an ecommerce sales chat platform to improve online customer experience

Advertising hosts

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
366	http://ib.adnxs.com	GET	/seg?add=95287&redir=http%3A%2F%...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	1002	HTML		
369	http://ads.yahoo.com	GET	/pixel?id=1643278&t=2&piggyback=http...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	230			
373	http://ib.adnxs.com	GET	/netuid2http://dis.criteo.com/dis/rb/app...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	753	HTML		
374	http://barnesandnoble.needle.com	GET	/pageupdate?vid=3b11-24498&pgid=2...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	285	script		
375	http://www.barnesandnoble.com	GET	/includes/check-login.jsp?_=148068901...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	513	script	jsp	
378	http://www.barnesandnoble.com	GET	/modals/account/login.jsp?parentUri=htt...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	715	text	jsp	
379	http://www.barnesandnoble.com	GET	/account/login-frame.jsp?tplName=login...	<input checked="" type="checkbox"/>	<input type="checkbox"/>			HTML	jsp	
380	http://pixel.rubiconproject.com	GET	/tap.php?v=5421&nid=2054&put=28183...	<input checked="" type="checkbox"/>	<input type="checkbox"/>			HTML	php	
381	http://static.criteo.net	GET	/empty.html	<input type="checkbox"/>	<input type="checkbox"/>			HTML	html	
382	http://barnesandnoble.needle.com	GET	/pageupdate?vid=3b11-24498&pgid=2...	<input checked="" type="checkbox"/>	<input type="checkbox"/>					

```
Request Response
Raw Params Headers Hex
GET /modals/account/login.jsp?parentUri=http%3A%2F%2Fwww.barnesandnoble.com%2F&tplName=login&_=0.3064351927217399 HTTP/1.1
Host: www.barnesandnoble.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Referer: http://www.barnesandnoble.com/
Cookie: JSESSIONID=51FC9E120701BA7403B991FEF5FAEC36.prodny_store01-atgap09; userPrefLanguage=en_US;
WZA=!BJJb5mhgha2Qh6ZLTQ+Tjs7s3ShelhbXCxGcQgJxyxeclUs9EwsdXAY6W+MxrcuLLwZ950t29EDBFA==; org-dc=WB; DeviceType=Desktop; showSiteAs=Desktop;
client-profile=Desktop;
TS01e75984=01b226976044b25e0bf3d20f31f699cb7690972e521d52dee46f83c5769d81ef2a92ald6a36d33a45acfb373b53bad08dc250b154ecc1ccbb41dc724cfc9f300
fbb92fe49f161593a22e1dadd54a3f162d21522315;
TS01af0a8e=01b2269760a52d844495eef8b4c197b4ef08f9f18862dfafbc02966fdafaf9295c3dfe58c539alclbcb42f4bba11356e7b40a2668cb30afd985425ae147fd17
6e1a3a212a30381ac7bd2087766c035630835e417407acc73091583d023c91a28f8a088839;
AMCV_9A223704532965F10A490D44*40AdobeOrg=-227196251*7CMCIDTS*7C17138*7CMCMID*7C42509705166738463899096276691228171750*7CMCAID*7CNONE*7CMCOP
TOUT-1480695737s*7CNONE*7CMCAAMLH-1481293337*7C7*7CMCAAMB-1481293337*7CcIBAx_aQzFEHcPoEvOGwcQ;
AMCVS_9A223704532965F10A490D44*40AdobeOrg=1;
mbox=session#1480688874651-889400#1480690860|PC#1480688874651-889400.17_13#1481898600|check#true#1480689060; fxmv=RENqpGfXwVsVkrOSS;
_ga=GA1.2.210199037.1480688881; _gat=1;
needlepin=N190d148068888182643b110011137bf644f27bf644f27bf6456a000000000000000117bf645620000000000000; setPrevPageName=Home;
s_vnum=1483246800568*26vn*3D1; s_invisit=true; s_depth=0; s_lv=1480689010897; s_lv_s=First*20Visit; s_cc=true;
```

Proxy Intercepting result: Create an account page

Advertising hosts

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	C
523	http://ib.adnxs.com	GET	/seg?add=95287&redir=http%3A%2F%...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	1002	HTML				<input type="checkbox"/>	68.67.180.44	a
528	http://sp.analytics.yahoo.com	GET	/spp.pl?a=10001287818027&.yp=3987...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	403		pl			<input type="checkbox"/>	98.139.225.35	
529	http://ads.yahoo.com	GET	/cms/v1?esig=1~7315a025058f312818...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	502	text				<input type="checkbox"/>	98.139.225.43	
530	http://ib.adnxs.com	GET	/getuid?http://dis.criteo.com/dis/rtb/app...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	753	HTML				<input type="checkbox"/>	68.67.180.44	s
533	http://trc.taboola.com	GET	/sg/criteo/1/rtb/	<input type="checkbox"/>	<input type="checkbox"/>	302	531					<input type="checkbox"/>	23.205.210.186	t
537	http://ads.yahoo.com	GET	/pixel?id=1643278&t=2&piggyback=http...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	230					<input type="checkbox"/>	98.139.225.43	
539	http://barnesandnoble.needle.com	GET	/pageupdate?vid=3b11-24498f&pgid=4...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	151	script				<input type="checkbox"/>	54.243.187.5	
540	http://www.barnesandnoble.com	GET	/modals/account/register.jsp?parentUrl...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	701	text	jsp			<input type="checkbox"/>	104.121.99.39	u
541	http://www.barnesandnoble.com	GET	/modals/account/register.jsp?parentUrl...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	701	text	jsp			<input type="checkbox"/>	104.121.99.39	u
542	http://www.barnesandnoble.com	GET	/modals/account/register.jsp?parentUrl...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	743	text	jsp			<input type="checkbox"/>	104.121.99.39	u

Request Response

Raw Params Headers Hex

```
GET /modals/account/register.jsp?parentUrl=http%3A%2F%2Fwww.barnesandnoble.com%2F&tplName=register&_=.9294277275895181 HTTP/1.1
Host: www.barnesandnoble.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Referer: http://www.barnesandnoble.com/
Cookie: JSESSIONID=51FC9E120701BA7403B991FEF5FAEC36.prodny_store01-atgap09; userPrefLanguage=en_US;
W2A=|BJfKbsmhgga2Qh6ZLTQ+Tjs7s3ShellhbXCxGcQgJxyxeclUs9EwsdXAY6W+MD;xucLLw2950t29EDBFA==; org-dc=WB; DeviceType=Desktop; showSiteAs=Desktop; client-profile=Desktop;
TS01e75984=01b226976071023e4603d708c7f15d0afd3e67697d77ca692366bc779d82dfe8e0490cf2a014d625f4daddb663d766029d4f13a046c10ba35505f0a44668b8489a0a07a64c28a250f2445fdb2c2fb480421e3fec8;
TS01af0a8e=01b2269760a52d844495eeff8b4c197b4ef08f9f18862dafa202966fdafaf29c5c3dfe58c539alc1bccc4b2f4bb1356e7b40a2668cb30afd985425ae147fd176e1a3a212a30381ac7bd2087766c035630835e417407acc73091583d023c91a28f8a088839;
AMCV_9A223704532965F10A490D4440AdobeOrg=-227196251*7CMCIDTS*7C17138*7CMCID*7C42509705166738463899096276691228171750*7CMCAID*7C0N0N*7CMCOPTOUT-1480695737s*7C0N0N*7CMCAAMLH-1481293337*7C7*7CMCAAMB-1481293337*7CcIBAx_aQzFEHcPoEv0GwcQ; AMCVS_9A223704532965F10A490D4440AdobeOrg=1;
mbox=session#1480688874651-889400#1480691162|PC#1480688874651-889400.17_13#1481898902|check#true#1480689362; fxmv=RENqGfXwVsvrOSS; _ga=GA1.2.210199037.1480688881; _gat=1;
needlepin=N190d148068888182643b110011157bf644f27bf644f27bf6469700000000000000000117bf645620000000000000; setPrevPageName=Home; s_vnum=1483246800568*26vm*3D1; s_invisit=true;
s_depth=18; s_lv=1480689368911; s_lv_s=First*20Visit; s_cc=true;
RT="s1=6&ss=1480688877791&tt=94370&obo=1&bcn=*2F*2F3211c0e1.mpst.at.us*2F&sh=1480689304313*3D6*3A1*3A94370*2C1480689299651*3D5*3A1*3A89712*2C1480689299517*3D4*3A1*3A41692*2C1480689002490*3D3*3A0*3A41692*2C1480688997175*3D2*3A0*3A37368&dm=barnesandnoble.com&si=03cae0ee-3e57-4a8b-a309-08052e6a9311&lId=1480689304314&nu=http%3A%2F%2Fwww.barnesandnoble.com%2F&c1=1480689371213";
s_sq=banqlobal*3D*2526c.*2526a.*2526activitymap.*2526page*253DHome*2526link*253DCreate*252520an*252520Account*2526region*253DmyAccountLinks*2526pageIDType*253D1*2526.activityvmap
```