

Weak session ids 발표

2026년 7월 15일 수요일 오전 10:42

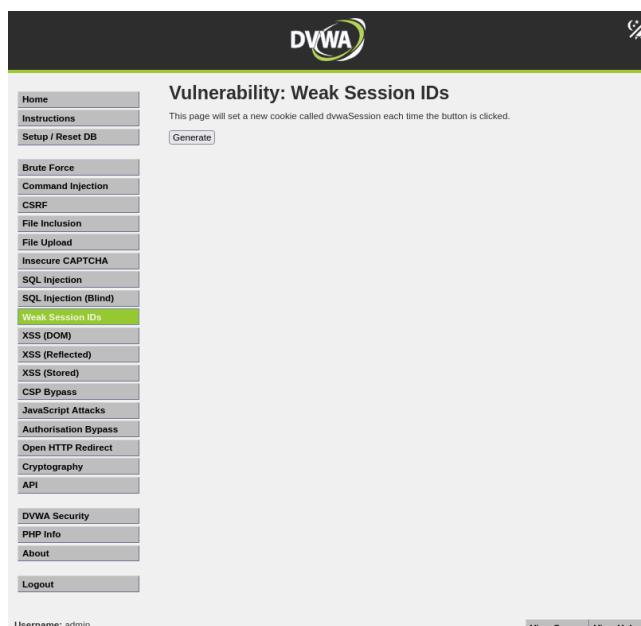
Weak session IDs란 말 그대로 취약한 세션 ID라는 뜻으로 세션의 아이디는 암호로서 복잡성을 만족해야 하는데 규칙성이나 예측이 쉬운 세션아이디를 발급해줌으로써 해커가 이를 알아내어 세션아이디가 탈취당하는 등의 취약점이 드러나는 해킹기법.

사용자가 웹사이트에 로그인을 하면 웹사이트에서는 세션id를 브라우저 쿠키에 저장해둠
이후 브라우저는 이 번호표를 서버에 보내서 로그인상태를 유지

여기서 weak의 의미

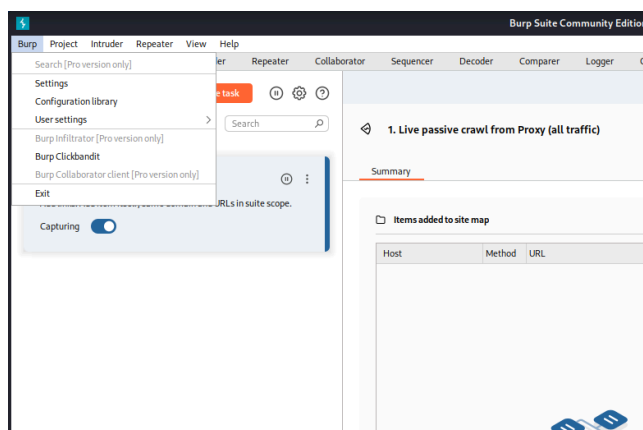
이 세션아이디는 아무도 예측할 수 없도록 랜덤하고 복잡해야 하지만 발급하는과정에서 일정한 패턴이 있는경우나 예측 가능한 값을 기반으로 만든경우 혹은 너무 길이가 짧을경우에 취약하다고 판단됨.

만약 공격자가 세션 아이디의 규칙을 파악하면 브루트포스와 같은 무작위 대입을 통해 현재 로그인된 세션 아이디를 알았을경우 아이디랑 비밀번호를 몰라도 사용자의 계정을 세션 하이재킹을 통해서 권한탈취 가능.

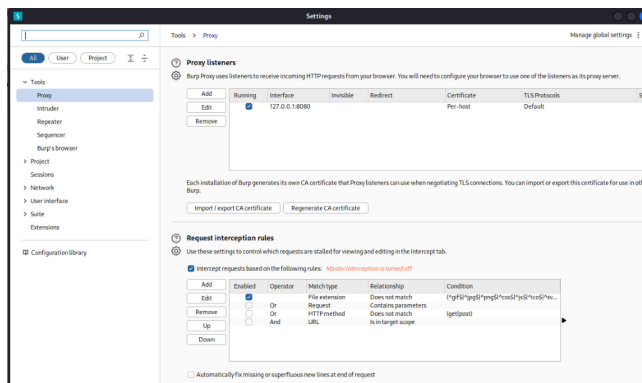


Dvwa의 weak session IDs 페이지

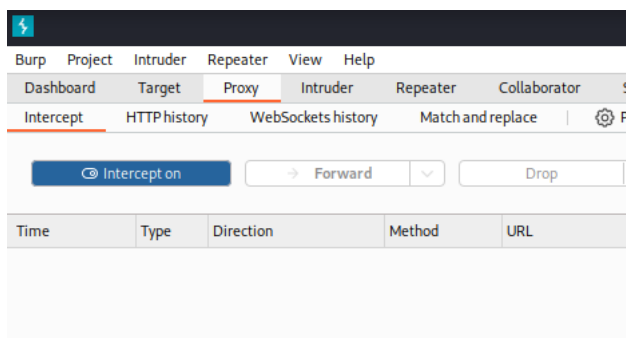
해당 페이지의 원래 용도는 사용자에게 세션을 식별할 수 있는 고유한 세션ID를 발급해주는 기능을 제공 일반적인 웹사이트는 로그인에 성공한 순간 서버가 세션 ID를 자동으로 발급해주지만 DVWA의 페이지는 버튼을 누르면 세션ID가 수동으로 발급되도록 만들어놓음.



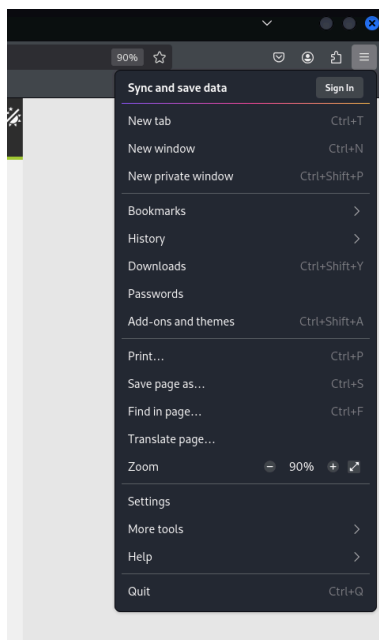
버프슈트로 해당 페이지의 동작을 확인해보기 위해 셋팅으로 가서 아이피 설정



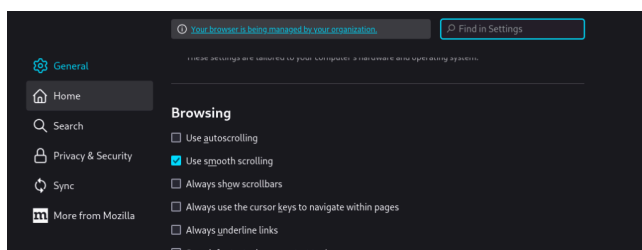
동작확인을 위해 공격자 자신의 세션아이디 확인만 하는거라 그냥 기본설정 그대로 놔둠

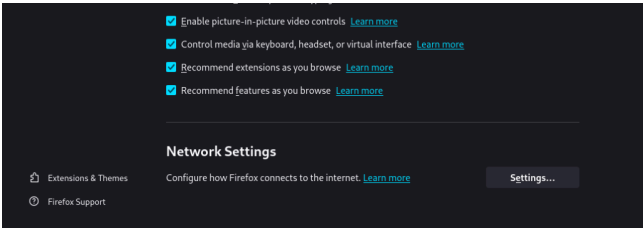


활성화 시켜줌.

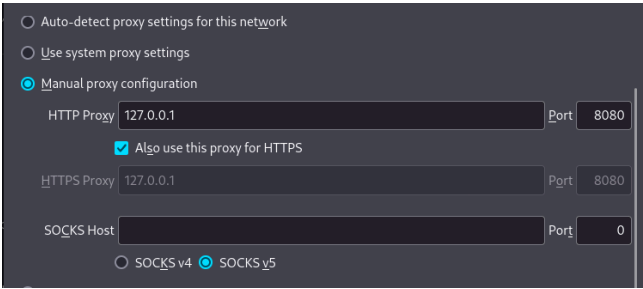


이제 파이어폭스로 와서 설정창에서 프록시 수동설정
여기서 세팅 클릭

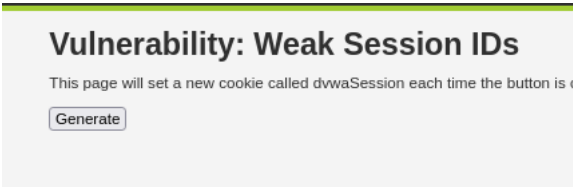




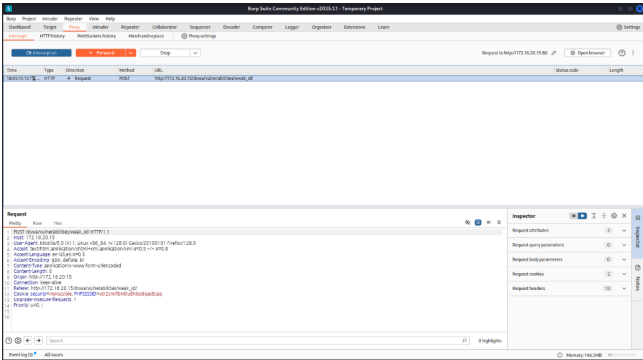
하단 맨 아래 내려와서 네트워크 세팅 들어가서 프록시 설정



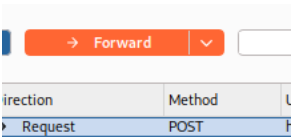
버프슈트에 설정한 127.0.0.1에 포트 8080으로 설정해주고 밑에 체크박스도 체크



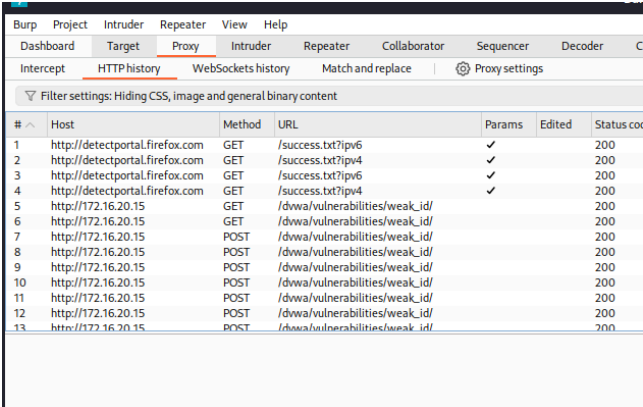
설정이 끝났으면 DVWA페이지로 돌아가서 버튼 클릭



보면 패킷잡은걸 볼 수 있음.

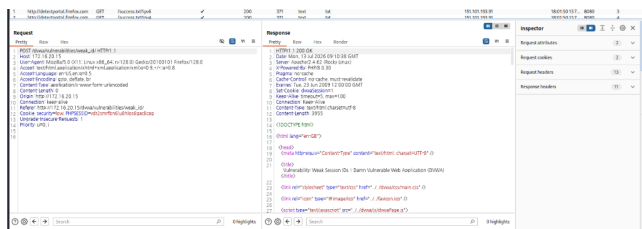


포워드 눌러주고



Http history 항목으로 들어옴.

#	Host	Method	URL	Params	Edited	Status code
1	http://127.0.0.1:8080	GET	/success.txt?ip=6			200
2	http://127.0.0.1:8080	GET	/success.txt?ip=4			200
3	http://127.0.0.1:8080	GET	/success.txt?ip=6			200
4	http://127.0.0.1:8080	GET	/success.txt?ip=4			200
5	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
6	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
7	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
8	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
9	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
10	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
11	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
12	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200
13	http://127.0.0.1:8080	POST	/vulnerabilities/weak_id/			200



세션항목 확인

```

Expires: Tue, 23 Jun 2009 12:00:00 GMT
Set-Cookie: dwwaSession=1
Keep-Alive: timeout=5, max=100
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Set-Cookie: dwwaSession=2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Set-Cookie: dwwaSession=3
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```

연속 세번 누른거로 세번 발급받은 값을 확인해보면 세션아이디가 1,2,3으로 숫자순으로 아주 단순한 방식으로 발급되는 취약점을 확인