|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성: 고승원 | | |  | |
|  | Broken Authentication | | | | | | |  |
|  | | Broken Authention | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. Broken Authentication 개요 |
| 1. Broken Authentication 이란  - 인증 및 세션 관리와 관련된 어플리케이션 기능이 종종 잘못 구현되어 공격자에게 취약한 암호, 키 또는 세션 토큰을 제공하여, 다른 사용자의 권한을 얻도록 착취하는 것을 말한다.  - 웹사이트에 가입할 때 추측할 수 있거나 무차별 대입 공격이 가능한 비밀번호 입력을 허용하는 경우도 포함됨.  2. Broken Authentication 특징   1. 하나가 뚫리면 모든 계정이 노출 될 수 있음 |
| 1. 안전하지 않은 로그인 형식 |
|  |
|  |
| 1. 안전하지 않은 로그인 형식 |
| - 웹페이지가 안전하지 않은 로그인 형식을 사용하는지 확인 |
| **① 난이도 하**  1-1) bee박스에 로그인    1-2) 로그인 후 Inseucure Login Froms 선택 후 Hack클릭    1-3) 로그인화면에서 오른쪽 클릭 후 Inspect Element클릭    1-4) font의 color 속성을 black으로 변경  - 로그인과 패스워드 옆에 아이디와 패스워드가 뜸    1-5) 옆에 있는 아이디와 패스워드를 입력한뒤 로그인 성공했는지 확인    **② 난이도 중**  2-1) medium으로 변경 후 set 클릭    2-2) 난이도 하와 같이 오른쪽 마우스 클릭 후 개발자도구 띄움  - 이번에는 패스워스가 font로 안써져 있음.    2-3) 이번에는 오른쪽 클릭 후 View Page Source 클릭  2-4) 코드 확인  - password의 값이 passphrase인데 만약 secret에 들어있는 값과 같으면 로그인 되게 되어있음.    2-5) 위에 변수들을 조합해 패스워드를 만든 뒤 로그인.  - charAt은 안의 숫자에 위치한 문자를 가져옴. (0부터 시작함)  - 변수 b는 h, 변수 j는 u 이런식으로 조합하면 됨. |
| 1. 무차별 대입 공격 |
|  |
| -기본적으로 개발자와 사용자 동일하지 않기에 관리자 패스워드의 변경 인터페이스가 별도로 만들어져 있지 않고, 데이터 베이스를 직접 변경하는 것과 같이 원시적인 형태를 갖는 경우가 많기 때문에 사용자는 최초 개발자가 설정해놓은 패스워드를 그대로 쓸 때가 많다. |
| **① 난이도 하**  1-1) burp suite를 킨 뒤 intercept is on를 off으로 바꿈.    1-2) firefox에서 맨 오른쪽 아이콘 클릭 후 Preferences 클릭    1-3) 맨밑의 네트워크 세팅 클릭    1-4) proxy칸에 127.0.0.1 설정 후 Port는 8080으로 설정    1-5) intercept is on으로 변경 뒤 내가 접속할 페이지 새로고침.  - burp suite에 잡히는지 확인    1-6) 로그인 후 Password Attacks 클릭    1-7) 가로챈 요청의 내용이 보이는 패널에서 오른쪽 클릭한 뒤 send to intruder 클릭.    1-8) Intruder 탭에 가서 하단의 새로 생긴 숫자 탭을 클릭.  - 왼쪽의 clear버튼 누른뒤 password자리에 add를 눌러 하단의 그림과 같이 추가.      1-9) payloads탭 클릭 후 Payload type을 Bruteforcer(무차별대입공격)으로 변경  - 하단에 min length와 max length 변경.(필자는 비밀번호가 bug인것을 알기 때문에  속도 때문에 b,g,u 만 검색하도록 조정함.)    1-10) positions 탭 클릭 후 start attack 클릭.  - start attack 클릭 시 공격 시작함.    - 공격 진행중 결과 값이 다른게 있을 경우 로그인에 성공하는 패스워드란 뜻이다.    1-11) 로그인 페이지에 가서 로그인 해보면 로그인 성공 된다고 뜬다. |
| 1. 사전 대입 공격 |
| - 무차별 대입 공격과 비슷해 보이지만 비밀번호를 설정하는 사람들이 선호하는 문자열을 대입하는 공격이다. |
| **① 난이도 하/중**  - FuzzDB를 이용하여 사전대입공격 진행. (FuzzDB는 퍼징에 사용되는 입력 값을 모은 데이터 베이스.)  1-1) FuzzDB다운로드  https://github.com/fuzzdb-project/fuzzdb  1-2) 압축해제  root@kali:~/Desktop /# unzip fuzzdb-master.zip  1-3) 가로챈 요청의 내용이 보이는 패널에서 오른쪽 클릭한 뒤 send to intruder 클릭.    1-4) 공격 타입을 Cluster bomb으로 변경 후 add와 clear버튼 이용해 추가.      1-4) Intruder탭으로 이동 후 페이로드 타입 simple list로 변경    1-5) payload option에서 load 클릭 후 zip파일 풀었던 곳에서 phpbb.txt선택.  - 위치 : fuzzdb-master/wordlists-user-passwd/passwds/phpbb.txt    1-6) Positions 탭으로 이동 후 start attack 클릭    1-7) length 값이 달라진 값을 확인 후 로그인 시도 |
| 1. Forgotten Function   - 비밀번호를 잃어버렸을 때 이메일로 비밀번호를 찾는 곳이다. |
|  |
| **① 난이도 하**  1-1) 먼저 비밀번호 힌트를 받을 이메일주소와 힌트를 적고 계정을 생성한다.    1-2) 생성한 계정의 이메일을 적고 비밀번호 힌트를 얻는다,    - 페이지에 힌트가 다 보인다.  ②난이도 중  - 난이도 중은 페이지에 힌트를 보여주진 않지만 해당 이메일로 힌트를 보내줌.  - 노란색 된 부분 코드는 이메일에 보내는 메시지 형식이다.  ‘    ③ 난이도 상  - 페이지에서 뜨는 메세지는 똑같지만 난이도 중과 달리 패스워드를 바꾸라고 메세지를 보낸다. |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
| 3. 결론 및 대응방법 |
| 1. 안전하지 않은 로그인 형식 |
| ① 웹 페이지 상에 아이디와 패스워드를 노출하지 않도록 만듬. |
| 1. 무차별 대입 공격 / 사전 대입 공격 |
| ① 캡챠를 입력하게 만듬.    ② 비밀번호를 최대한 어렵게 만들면 됨. |
| 1. Forgotten Function |
| ① 비밀 번호를 못찾을 시 변경 요청을 해당 이메일로 보냄. |
|  |
|  |