http://stolenbyte.tistory.com/44

Vuln 100

MP3 TAG내용으로 인해 SQL Injection 됨.
TAG<? system[$_GET['cmd']] ?> ~~~~~

그뒤 내용 넣고 올리면 파일주소에 ?cmd=ls하면 쉘이 실행 됨.
그러나 파일을 다 집어까도 패스워드는 없고, MySQL root 비밀번호 알수 있음.
그걸로 MySQL 접속.. 그전에 웹쉘 올려야하는데 올리때 TAG 전에 웹쉘 심고 올리면 웹셀 쓸수 있다.
그걸로 MySQL 접속한 뒤,
use music;
show table;

하면 vul100pwd라는 테이블 존재
select * from vul100pwd

끝

Binary 100

파일내용이 이상하다.
UUEncode란걸 이용하여 어느정도 알아 볼수 있는 자바스크립트 형태로 돌린다.

_$_$$_$="charAt";$=~[];$={___:++$,$$$$:(![]+"")[_$_$$_$]($),__$:++$,$_$_:(![]+"")[_$_$$_$]($),_$_:++$,$_$$:({}+"")[_$_$$_$]($),$$_$:($[$]+"")[_$_$$_$]($),_$$:++$,$$$_:(!""+"")[_$_$$_$]($),$__:++$,$_$:++$,$$__:({}+"")[_$_$$_$]($),$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[_$_$$_$]($.$_$)+($._$=$.$_[_$_$$_$]($.__$))+($.$$=($.$+"")[_$_$$_$]($.__$))+((!$)+"")[_$_$$_$]($._$$)+($.__=$.$_[_$_$$_$]($.$$_))+($.$=(!""+"")[_$_$$_$]($.__$))+($._=(!""+"")[_$_$$_$]($._$_))+$.$_[_$_$$_$]($.$_$)+$.__+$._$+$.$;$.$$=$.$+(!""+"")[_$_$$_$]($._$$)+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$$$_+"\\"+$.__$+$.$$_+$.$$_+$.$_$_+(![]+"")[_$_$$_$]($._$_)+"("+$.$$$$+$._+"\\"+$.__$+$.$_$+$.$$_+$.$$__+$.__+"\\"+$.__$+$.$_$+$.__$+$._$+"\\"+$.__$+$.$_$+$.$$_+"(\\"+$.__$+$.$$_+$.___+","+$.$_$_+","+$.$$__+",\\"+$.__$+$.$_$+$._$$+","+$.$$$_+",\\"+$.__$+$.$$_+$._$_+"){"+$.$$$_+"=\\"+$.__$+$._$_+$._$$+$.__+"\\"+$.__$+$.$$_+$._$_+"\\"+$.__$+$.$_$+$.__$+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.$__+$.$$$+";\\"+$.__$+$.$_$+$.__$+$.$$$$+"(!''.\\"+$.__$+$.$$_+$._$_+$.$$$_+"\\"+$.__$+$.$$_+$.___+(![]+"")[_$_$$_$]($._$_)+$.$_$_+$.$$__+$.$$$_+"(/^/,\\"+$.__$+$._$_+$._$$+$.__+"\\"+$.__$+$.$$_+$._$_+"\\"+$.__$+$.$_$+$.__$+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.$__+$.$$$+"))){\\"+$.__$+$.$$_+$.$$$+"\\"+$.__$+$.$_$+$.___+"\\"+$.__$+$.$_$+$.__$+(![]+"")[_$_$$_$]($._$_)+$.$$$_+"("+$.$$__+"--)\\"+$.__$+$.$$_+$._$_+"["+$.$$__+"]=\\"+$.__$+$.$_$+$._$$+"["+$.$$__+"]||"+$.$$__+";\\"+$.__$+$.$_$+$._$$+"=["+$.$$$$+$._+"\\"+$.__$+$.$_$+$.$$_+$.$$__+$.__+"\\"+$.__$+$.$_$+$.__$+$._$+"\\"+$.__$+$.$_$+$.$$_+"("+$.$$$_+"){\\"+$.__$+$.$$_+$._$_+$.$$$_+$.__+$._+"\\"+$.__$+$.$$_+$._$_+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.$__+$.___+"\\"+$.__$+$.$$_+$._$_+"["+$.$$$_+"]}];"+$.$$$_+"="+$.$$$$+$._+"\\"+$.__$+$.$_$+$.$$_+$.$$__+$.__+"\\"+$.__$+$.$_$+$.__$+$._$+"\\"+$.__$+$.$_$+$.$$_+"(){\\"+$.__$+$.$$_+$._$_+$.$$$_+$.__+$._+"\\"+$.__$+$.$$_+$._$_+"\\"+$.__$+$.$_$+$.$$_+"'\\\\\\\\\\\\"+$.__$+$.$$_+$.$$$+"

위에 처럼 나옴
저부분을 alert 찍어보면
CodeGate_JavaScriptEncode_Key = "120a151156120a163t111163120lea163u162e!"

http://stolenbyte.tistory.com/44

이렇게 뜸

숫자부분 7진수 이던가 그럴거임
풀면 PainPastIsPleasure! 이렇게 됨
우리팀원이 풀어서 정확한지는 100% 장담 못함.

끝

Crypto 100

이미지 숫자를 그대로 휴대폰 자판으로 따라 치면 패스워드 나옴.
제일 마지막에 잇는 keypad cipher가 답

끝

forensic 100

파일 내부에 있는 zip을 다 뺀다.
그 중에 하나는 xls파일임
그 파일 압축을 풀면 index.xml이라고 잇슴
거기에 base64된것을 바이너리 형태로 디코딩 하면 png파일이 나옴
그게 답

끝

network 100

pcap파일인데, 통신한 모든 파일 다 추출함.
그러고 보면 HA1A인가 하는 지뢰찾기 파일이 하나 보임
유일한 PE포맷을 가진 파일임
그거 MD5 해쉬해서 인증 하면 됨

끝

issue 100

동영상 파일인데, 동영상 내에 GPS 위치 뺌.
구글 지도로 찍어본다. 위치가 답
정확한지 모름. 같이 하는사람이 풀음.

끝

vuln 200

모든 SQL Injection이 가능함. 그러나 Administrator가 아니면 다 낚시임. 패스워드가 있는 데이터베이스를 쓸 수가 없음.

http://stolenbyte.tistory.com/44

Administrator로 로그인하고 소스 보기하면 <!-- hint 1 -->
유일하게 1이라고 찍힌다. 다른건 다 0
쿠키를 보면 lang이라고 잇는데 그부분이 SQL Injection이 된다.
그래서 raw_data라는 테이블 다 까면
유일하게 눈에 딱 튀는 base64문장이 잇음.
그거 바이너리 형태로 디코딩하면 답이 있음.

끝

binary 200

상당히 어이없던 문제엿음.
1분만에 해결 가능한건데, 그냥 f8 누르다가 http 주소하나가 뜸.
그게 답.

끝

crypto 200

비즈네르 암호.
대신 답이 평문에서 암호만들때 사용되는 키가 답.
그러나 구글검색하면 다 찾아준다.
키 길이가 6이라서.. 홈페이지에 대부분 애들이 기본 베이스가 5인데 6으로 해주니 바로 답주더라.

끝

forensic 200

빡쳐서 죽을뻔한 문제.
jpg 다 뺀다. the key ~~ 한 그림이 썸네일과 잇는데 큰 그림은 답부분이 짤림.
쫑트 빡침.
섬네일은 사신의 눈아니면 못봄
그래서 빡쳐잇는중에 jpg는 제일 마지막에 FF D9가 들어감.
엄청 밑부분에 그게 잇길래 the key~~ 이 그림이랑 합치니깐 그림이 보임

끝

network 200

언뜻보면 할말없는 깨끗한 pcap파일임
그러나 힌트로 xor하라고 함.
127.0.0.1 잡힌부분 xor 하면 되는데 xor키가 게씽한듯?
그러면 문자열이 나오는데 그게 답.
몇개 나온걸로 기억

끝

http://stolenbyte.tistory.com/44

issue 500

대회 중에 가장 제일로 빡친 문제
문제 다 박살 내버리고 싶엇슴.
hint로 SMS가 뜸.
그래서 framework를 디코딩함.
그래서 보니 a1, a2함수가 잇슴.
거기서 비교하는게 잇는데 그 숫자를 다 모앗슴.
난 이게 답인줄 알앗는데, 답이 아님
또 빡침

잠 24시간 이상 못잔상태라 상태가 호구임.
암튼 알고보니깐 위에 GSM 7bit Encode라는게 잇네?
아오 그래서 Decode Python으로 된거 구함.
디코딩햇는데 평문 안보임 ㅋㅋ
이게 머임??ㅋㅋㅋㅋㅋㅋㅋ
더더욱 빡침

같이 하는분이 삽질하다가 다 더해봄.
아놔 풀리네? 답이 요기잉네

이런

끝

vuln 300

이건 좀 웃기게 풀엇슴.
남들 열심히 풀때 난 history 열심히 보고 잇엇슴
history에 먼가 코드처럼 보이는게 찍히더니
그게 하루종일 돌려놓고 잇더니 쉘 뜨네요.

끝

binary 300

BHO 파일임.
그거 regsvr32로 등록시킴
그럼 IE에 붙음
거기 보면 인코딩하는 함수가 너무 눈에 잘띔
그부분 호출하는부분이 총 3군데 인데
그중 제일 밑에는 어떻게든 안가더라
그래서 강제 점프시켜서 돌리니깐 답이 뜨네.

끝

http://stolenbyte.tistory.com/44

forensic 300

이건 툴한방이면 다 풀림.
http://www.forensicswiki.org/wiki/USB_History_Viewing
Windows USB Storage (USBSTOR) Parser라는 툴이 잇슴
나도 이거 썻는데 어떤 외국팀도 이거 썻던데 암튼 좋음.
그래서 이걸로 패스워드로 원하는 자료 다 찾음.

끝

network 300

이거 처음에 M만 찍어주니깐 대체 뭐냐 햇는데
똑같은 세션에 아이피 계속 바꿔주면서 보내면 답을 보냄
난 프록시 씀

끝

issue 300

이거 뭐 QR코드 복구 해주는 프로그램이 잇는데
그게 돌리니깐 답 줌.

끝

vuln 400

우리 팀원이 풀어서 기억이 안남.

끝

binary 400

PE 섹션을 다 나눠서 줌.
근데 중요한건 PE헤더가 업슴 ㅠㅠ
팀원 한명이 삽질하면서 PE헤더 만들엇슴
실행시키니깐 다이얼로그에 답

근데 팀원이 자꾸 실행 안된다고 질질 짬
그래서 내가 섹션 보니깐 권한을 왜 안줌?ㅋ

끝

crypto 400

http://stolenbyte.tistory.com/44

이거 오라클 패딩인데, 이거 그전까진 패딩 맞추는 잉여짓 함.
구글검색하다가 200, 403, 500에 관련된 오라클 패딩 보게 됨.
그래서 오라클 패딩 문서 보고 풀이하니깐 답 뜸.

다 쓸라면 너무 김.
귀찮

끝

issue 400

그림이라고 함. 근데 다른 hex는 이미지 인거 같은데 헤더가 전혀 듣보잡임.
근데 헤더쪽에 보면 ^ CODH이라는게 보임
그래서 CODH로 xor해보니깐 PNG 헤더 비슷한게 보임
그래서 CODA~하다가 CODE에서 답 뜸.

끝

issue 500

키보드 입력 받는 걸 해쉬하는 루틴이 있고
그 루틴을 때내서 C로 재구성해서 0x2002가 맞게 해야함.
키보드 입력을 16개를 받아서 그거랑 맞으면 키값을 뱉는데
근데 경우에수가 많아서 웹에다 그 키를 넣으면 답이 나오도록 문제를 수정 함.

참고로 0x2002가 되면 컴터를 부팅해주는 코드
같이 풀엇던 사람인데 소스 안주셧슴.
덕분에 .. ㅋㅋㅋㅋ

끝