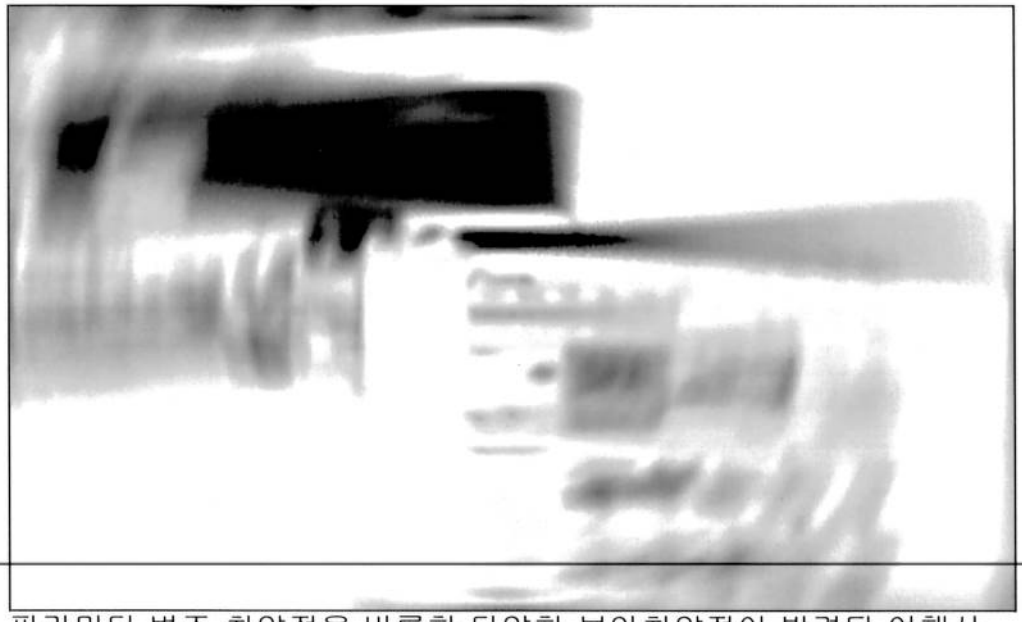
보안뉴스 미디어

여행사 웹사이트 관리자 페이지, 해커 맘대로 들락날락?

2012-09-25

T사 및 G사 여행사 사이트에서 보안취약점 잇따라 발견!
여행상품 가격 변경은 물론 웹쉘 삽입 등으로 권리자 권한 탈취 가능

[보안뉴스 권 준] 오는 9월 29일부터 추석명절과 개천절을 잇는 황금연휴가 시작됨에 따라 해외 휴양지를 비롯해 국내외 여행을 계획하는 사람들이 부쩍 많아지고 있다. 이에 대목을 맞은 국내 여행사들도 각종 패키지 여행상품을 개발해 홈페이지에 게시하면서 소비자들의 관심을 유도하고 있다.



파라미터 변조 취약점을 비롯한 다양한 보안취약점이 발견된 여행사 사이트 2곳

이렇듯 황금연휴를 앞두고 최근 방문자수가 많아지고 있는 여행사 웹사이트에서 파라미터 변조 취약점을 비롯한 각종 보안취약점이 잇따라 발견돼 여행사들의 홈페이지 관리가 매우 허술한 것 아니냐는 지적이 제기되고 있다.

특히, 악의적인 해커들이 파라미터 변조 취약점을 악용할 경우 관리자 페이지에 마음대로 접속해 관광상품 가격 등의 정보를 변경하는 것은 물론 여행사 회원들의 개인정보 탈취가 가능해 큰 피해가 발생할 수 있다. 더군다나 전문기술을 보유하지 않더라도 너무나 손쉬운 방법으로 관리자 페이지에 접속 가능하다는 게 더욱 큰 문제다.

이러한 여행사 웹사이트들의 보안취약점을 본지에 제보한 청소년 해킹·보안팀 Little Rascal의 리더 염세현 군에 따르면 별도의 인증정보 없이 관리자 홈페이지에 접속이 가능해 악의적인 해커가 관리자처럼 각종 여행정보나 공지사항 등을 마음대로 변경할 수 있다는 것. 이를 통해 여행사는

물론 소비자들에게도 물질적 피해를 끼칠 수 있기 때문에 여행사 측의 신속한 조치가 필요하다는 지적이다.

우선 T여행사 사이트의 경우 다양한 여행상품을 제공하는 사이트로 많은 사용자들이 접속하는 여행사이트 가운데 하나인데, 사용자 로그인과 함께 관리자 로그인 페이지로 손쉽게 이동 가능하다. 여기서 파라미터 값을 유추해 관리자 폴더 명을 입력하면 별도의 관리자 인증 없이 관리자 페이지로 넘어갈 수 있다는 것.

이는 다시 말하면 정상적인 관리자 계정과 암호를 사용해 인증을 받았는지 확인하는 프로세스가 누락되어 별도의 인증정보 없이 관리자 페이지로 접근할 수 있다는 얘기다.

이를 통해 악의적 해커가 관리자 페이지에서 활동할 수 있게 되면 여러 가지 피해가 발생할 수 있다. 일례로 해커가 여행상품의 가격을 터무니없이 저렴하게 고쳐놓을 경우 이를 보고 소비자들이 해당상품을 신청하게 되면 추후 큰 분쟁의 소지가 생길 수 있다.

지난 5월 ABC마트 홈페이지에서 시스템 오류로 전 상품의 가격이 39,000원으로 표기돼 이를 보고 구매한 소비자와 ABC마트 사이에 한바탕 소동이 발생한 적이 있었는데, 여행사 웹사이트에서도 이러한 사례가 재발될 수 있는 셈이다.

더욱이 T사이트의 경우 이미지 업로드를 통해 얼마 전 EBS 해킹으로 이슈가 된 웹쉘 업로드가 가능하고 구글링을 통해 웹사이트 관리자 계정이 노출돼 있다는 점도 지적됐다. 이와 관련 염 군은 "웹쉘이 업로드 될 경우 무엇보다 관리자의 정확한 아이디 및 패스워드를 확인할 수 있고, 홈페이지 전체를 컨트롤 할 수 있다"며, "더욱 심각한 건 XSS나 iframe 등의 악성 해킹기법을 통해 접속자 모두에게 피해를 주는 최악의 상황이 발생할 수도 있다는 점"이라고 우려했다.

또 다른 여행사인 G사 사이트에서도 파라미터 변조 취약점이 발견됐다. G사 사이트 역시 T사와 마찬가지로 관리자 페이지에 손쉽게 접근이 가능하고, 이를 바탕으로 해커가 관리자 게시글에 웹쉘 등을 삽입하거나 iframe, XSS 등의 해킹 기법으로 웹사이트 방문자의 악성코드 감염을 유도할 수 있는 것이다. 또한, 이 사이트에서도 구글링 취약점이 발견된 것으로 나타났다.

이에 본지는 보안취약점이 발견된 2곳의 여행사에 취약점에 대해 통보하고, 신속한 조치를 요청했다. 이와 관련 G사의 경우 웹 관리자가 공석인 상태로 알려져 웹사이트 관리가 허술했던 것으로 보이며, T사도 보안관리의 소홀함을 인정하며, 바로 조치를 취할 것을 약속했다.

이러한 보안취약점의 해결방안과 관련해 염 군은 우선 구글링 방지를 위해서는 웹사이트의 최상위 주소에 robots.txt를 추가시키고, robot.txt에는 아래와 같은 내용을 첨부할 것을 당부했다.

```
User-agent: *
Disallow: /
```

또한, 각종 보안취약점 예방을 위해 가급적 웹 방화벽을 사용하는 것이 바람직하다는 점도 강조했다. 웹 방화벽 도입비용이 당장 부담된다면 시중에 나와 있는 무료 웹 방화벽이라도 우선적으로

도입할 필요가 있다는 것.

이와 함께 외부에서의 관리자 페이지 접근을 차단하기 위해 관리자 자신의 IP만 허용하고 외부 IP 접속을 차단하거나 웹사이트 내에 관리자만 접근할 수 있는 해당 디렉터리에 외부자가 접근하면 로그인 페이지를 띄워서 접속을 차단하는 방법도 있다고 염 군은 밝혔다.

특히, 여행사 사이트의 경우 황금연휴를 앞두고 인터넷 사용자들의 방문이 크게 늘어나고 있는 만큼 웹사이트 보안관리에 만전을 기할 필요가 있다. 만에 하나 해커에 의해 사이트 관리자 권한을 탈취 당했을 때 입게 될 수 있는 여행사와 이용자의 피해가 막대한 만큼 보다 철저한 웹사이트 모니터링과 보안취약점 점검작업이 이루어져야 할 것으로 보인다.

한편, 이번 보안취약점을 본지에 제보한 청소년 해킹·보안팀 Little Rascal (littlerascal.tistory.com)은 리더 염세현 군을 중심으로, 강남훈, 성원영, 김정민 등 총 4명의 경주 월성중학교 학생들로 구성돼 있으며, 보안취약점 점검 활동 등을 통해 국내 보안의식 제고에 기여하고 있다.

[권 준 기자(editor@boannews.com)]