

[Hacker Factory] 웹워게임 1,2,3번

-1번

• 나의 포인트 : 0 POINT



슈퍼 파워 컴퓨터

- 제조사 : Hacker Factory
- 성능 : 세계 최강
- 가격 : 1,000,000,000 POINT

구매하기



스마트 게임기

- 제조사 : Hacker Factory
- 구성 : 게임기 1EA, 패드 2EA
- 가격 : 5,000,000 POINT

품절



디바블농7 확장팩

- 제조사 : Hacker Factory
- 구성 : Blue-Ray 2CD
- 가격 : 1,000,000 POINT


구매대기

최초 접속 화면이다.

슈퍼 파워 컴퓨터 구매하기 버튼을 눌러봤다.

상품 구매 페이지

슈퍼 파워 컴퓨터



- 제조사 : Hacker Factory
- 성능 : 세계 최강
- 구성 : 모니터 & 데스크탑(일체형), 키보드, 마우스, 각종 케이블
- 원가 : 5,000,000,000 POINT
- 할인율 : 80%
- 가격 할인가 : 1,000,000,000 POINT

즉시구매 닫기

위와 같은 모달창이 떴는데 즉시구매를 눌러봤다.

경고 : 결제 금액 부족

사용자의 포인트가 부족합니다. 확인해주세요.

×

슈퍼 파워 컴퓨터

• 제조사 : Hacker Factory

• 성능 : 세계 최강

• 가격 : 1,000,000,000 POINT

구매하기

스마트 게임기

• 제조사 : Hacker Factory

• 구성 : 게임기 1EA, 패드 2EA

• 가격 : 5,000,000 POINT

품절

디바블론7 확장팩

• 제조사 : Hacker Factory

• 구성 : Blue-Ray 2CD

• 가격 : 1,000,000 POINT

구매대기

위와 같은 경고 페이지가 뜬다.

모달 창에서 f12로 페이지 소스를 봤다.

```

▼<div class="modal-body">
  ▼<form name="Goods1" action="index.php" method="post">
    <input type="hidden" name="GoodsCode" value="1111111">
    <input type="hidden" name="UserPoint" value="0">
    <input type="hidden" name="Mode" value="Buy">
    <h4 class="media-heading">슈퍼 파워 컴퓨터</h4>
    
  
```

구매 정보 관련 form태그

```

▼<div class="modal-footer">
  ::before
  <button type="button" class="btn btn-primary btn-sm"
  onclick="if (!window.__cfRLUnblockHandlers) return false; do
  cument.Goods1.submit())">즉시구매</button> == $0
  <button type="button" class="btn btn-default btn-sm" data-
  dismiss="modal">닫기</button>
  ::after
  
```

즉시구매 버튼

여기서 UserPoint를 조작할 수가 있다. 충분한 금액 입력 후 버튼을 눌러봤다.

정상 결제 완료

정상적으로 결제가 완료되었습니다.

×

인증키 : SL07HQZ17ICiW39+2pGMF1rKID0YgWFh

성공

-2번

파격할인

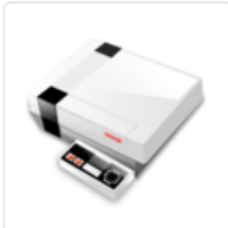
40% 이상의 할인가로 판매합니다!



슈퍼 파워 컴퓨터

- 제조사 : Hacker Factory
- 성능 : 세계 최강
- 가격 : 5,000,000원

상세보기



스마트 게임기

- 제조사 : Hacker Factory
- 구성 : 게임기 1EA, 패드 2EA
- 가격 : 5,000,000원

목적

2번 문제는 접속 시 이렇게 뜬다. 상세보기로 컴퓨터를 보자

파격할인

40% 이상의 할인가로 판매합니다!

슈퍼 파워 컴퓨터

제조사 : Hacker Factory

성능 : 세계 최강

구성 : 모니터 & 데스크탑(일체형), 키보드, 마우스, 각종 케이블

원가 : 10,000,000 원

판매가 : 5,000,000 원 (50% 할인)

배송비 : 0 원

구매하기

목록

상세보기에서 구매 관련 정보를 띄운다.

HACKTORY PAY

> Hacktory의 간편 결제 시스템

저희 **HackerFactory**에서는 자체 결제 시스템을 도입하여 결제 시 간편하게 결제를 할 수 있습니다.

결제 선택

- ☐ 휴대폰 간편결제
- ☐ 신용카드 간편결제
- ☐ 무통장입금 결제
- ☐ 실시간 계좌이체

다음

결제취소

구매하기를 누르면 결제 방법을 고를 수 있고

결제 선택 / 휴대폰 간편 결제

이름

이름을 입력하세요

통신사 선택

선택

휴대폰 번호

휴대폰 번호를 입력하세요

"-" 를 포함한 휴대폰 번호를 입력해주세요.

결제 금액

5,000,000원

해당 금액이 최종 결제 금액 입니다.

결제하기

이전

최종 결제 화면인데 결제 금액을 조작 할 수가 없다.

아무래도 구매 정보를 띄우는 곳에서 결제 금액을 조작해야 할 것 같다.

```
▼<form name="GoodsInfoForm" action="PaymentStep1.php" method="POST">
  <input type="hidden" name="GoodsCode" value="3012383">
  <input type="hidden" name="OriginalCost" value="10000000">
  <input type="hidden" name="CostDC" value="5000000">
  <input type="hidden" name="GoodsCnt" value="1">
  <input type="hidden" name="DeliveryCost" value="0">
  <input type="hidden" name="DeliveryFreeFlag" value="Y">
  <input type="hidden" name="TotalCost" value="5000000">
</form>
::after
```

F12로 구매 관련 정보를 볼 수 있다. 저기서 origincost와 totalcost를 조작해서 0 원으로 만들겠다.

결제 선택 / 휴대폰 간편 결제

이름

이름을 입력하세요

통신사 선택

선택

휴대폰 번호

휴대폰 번호를 입력하세요

"-" 를 포함한 휴대폰 번호를 입력해주세요.

결제 금액

0원

해당 금액이 최종 결제 금액 입니다.

결제하기

이전

조작했더니 성공적으로 0원으로 나온다.

정상 결제 완료

×

정상적으로 결제가 완료되었습니다.

인증키 : Q41dgtakfPGYL6+dTq03YTJ/t/tL27u/

성공

-3번

접속 화면이랑 구매까지 2번과 동일하다 form태그도 동일해서 2번과 같은 방식으로 해봤다.

hackerfactory.co.kr 내용:

상품 금액이 일치하지 않습니다.

확인

가격을 바꾸고 구매하기를 눌렀더니 이런 오류 메시지가 뜬다.

결제 페이지에서 f12로 코드를 유심히 보다 보면

```
▼<form name="Payment" action="PaymentStep2.php" method="POST">
  ▼<div id="content" class="modal-body">
    <input type="hidden" name="GoodsCode" value="3012383">
    <input type="hidden" name="OriginalCost" value="10000000">
    <input type="hidden" name="CostDC" value="5000000">
    <input type="hidden" name="GoodsCnt" value="1">
    <input type="hidden" name="DeliveryCost" value="0">
    <input type="hidden" name="DeliveryFreeFlag" value="Y">
    <input type="hidden" name="TotalCost" value="0zHXXdR1VXk=="> == $0
    <input type="hidden" name="PaymentAction" value="Y">
```

이렇게

숨겨진 form태그를 확인할 수 있다. 여기 값을 수정해주면 될 것 같다.

TotalCost의 값이 base64로 인코딩 되어 있다. 이걸 2번 디코딩하면

1]uUy

For encoded binaries (like images, documents, etc.) use the file upload

UTF-8

▼

Source character set.

☐

Decode each line separately (useful for when you have multiple entries)

☒

Live mode OFF

Decodes in real-time as you type or paste (supp

<

DECODE

>

Decodes your data into the area below.

2

이렇게 2라는 값이 나온다.

TotalCost에 2를 넣어주고 나머지 가격을 바꿔서 구매해봤다.

정상 결제 완료

정상적으로 결제가 완료되었습니다.

인증키 : BXMpXss1CFSxsJKfvPEnqe92o3s1XVJg

성공