Web Architecture 253

Privacy & Security

who's this guy?

columbia university

school of engineering and applied science

bs in computer science

1999

who's this guy?

13+ years
writing software and managing engineers

who's this guy?

4 months zynga

We all make mistakes

who's this guy?

ivan leichtling
engineering manager for
yelp's security team

what are we up to

- **why security matters**
- what's worth protecting
- principles of security
- common exploits
- security resources

why security matters

impact to business continuity

why security matters

impact to business continuity

why security matters

focus on security
to ensure
business continuity

why security matters

impact to finances

why security matters

impact to finances

Hackers steal money from trucking

22 November 2012 Last updated at 11:33 ET

1.7K Share

Anonymous hackers 'cost PayPal £3.5m'

Print Font Size:

A student attacked the PayPal website as part of a concerted effort by the Anonymous "hacktivists" that cost the company £3.5m, a court has heard.

Christopher Weatherhead, 22, was studying at Northampton University when he allegedly took part in the campaign

28, 2012.

The court heard
companies who
later attacked Pa
Wikileaks payme

Hacker steals $150,000 from school district payroll account

Print

November 27, 2012 7:39 pm • By ROD STETZER and ALICIA YAGER | The Chippewa Herald

why security matters

focus on security
to protect
your finances

why security matters

impact to your users

why security matters

impact to your users

Millions of South Carolina residents' data

attack against

to a single

Mistakes: South Carolina Gov. Nikki Haley, with investigator Mark Keel, admits the state's Department of Revenue did not do enough to protect sensitive data of millions of residents

Man arrested in Athens over ID theft of most of Greek population

Reuters – Tue, Nov 20, 2012

Hackers steal credit card data from 63 Barnes & Noble retail stores

By Shawn Knight
On October 24, 2012, 12:00 PM EST

3

why security matters

focus on security
to protect and maintain
your users

what are we up to

- why security matters
- **what's worth protecting**
- principles of security
- common exploits
- security resources

what's worth protecting

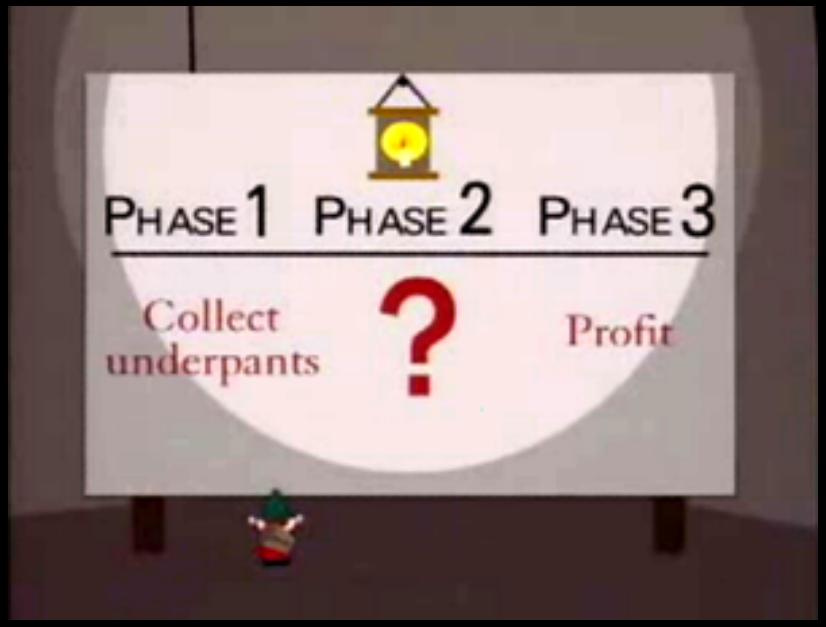
the first step in being a hacker is deciding what's worth stealing

the first step in security is deciding what's worth protecting

what's worth protecting

when you try to figure out what to protect
ask yourself the question

if i stole this, what could i do with it?



what's worth protecting

if i stole this, what could i do with it?

what's worth protecting

if i stole this, what could i do with it?

State	CompanyName	ADDRESS	City	ZIP	County	PHONE	FAX	ContactName	Title	Emp	YR Start	SALES	Code	Industry	Latitude	Longitude
GA	CLARKSTON INTERNATIONAL BIBLE CH	3895 CHURCH STREET	CLARKSTON	30021	DEKALB	4042966483	4042963902	DR B J BENNET	Co-Owner	16	1883	$410,000	8661	RELIGIOUS C	33.80787	-84.23908
GA	KOHL MARKETING, INC	1103 BOMBAY LN	ROSWELL	30076	FULTON	8003335645	4135321553	PAUL K. ENGLERT	Executive D	12	1990	$18,000,000	8742	MANAGEMEI	34.02489	-84.31191
GA	BARRY DESIGN INC	6375 SPALDING DRIVE SUITE B	NORCROSS	30092	GWINNETT	7705829000	7705821044	PATRICK BARRY	Co-Owner	4	1997	$210,000	8712	ARCHITECTU	33.96815	-84.22679
GA	MOUNT HOLLY CHURCH OF GOD	4685 NORTH HIGHWAY 27	CARROLLTON	30117	CARROLL	7705373370	7705370380	EVETT GUYTON	Co-Owner	5	1975	$150,000	8661	RELIGIOUS C	33.57676	-85.13293
GA	ALLATOONA LANDING MARINE RESOR	24 ALLATOONA LANDING ROAD	CARTERSVILLE	30121	BARTOW	7709746089	7709746143	MICHAEL SACJS	Co-Owner	29	1987	$1,700,000	7033	RECREATIOI	34.20216	-84.77766
GA	ASH STREET BAPTIST CHURCH KINDER	5370 ASH STREET	FOREST PARK	30297	CLAYTON	4043631989	4043611558	KEN CARTER	Co-Owner	6	1954	$180,000	8661	RELIGIOUS C	33.61035	-84.35906
GA	ST LUKE'S PRESBYTERIAN CHURCH	1978 MOUNT VERNON ROAD	ATLANTA	30338	DEKALB	7703931424	7703933278	CHRISTOPHER PRIC	Co-Owner	6	1969	$180,000	8661	RELIGIOUS C	33.94472	-84.31806
GA	TEMPLE DELIVERANCE	249 WADDELL STREET	ATHENS	30605	CLARKE	7065465510	7065465510	RUFUS ADDISON	Co-Owner	1	1983	$36,000	8661	RELIGIOUS C	33.90316	-83.32293
GA	NEW ELIM BAPTIST CHURCH	4368 HARTLEY BRIDGE ROAD	MACON	31216	BIBB	4787887575	4787884355	HERSCHEL SEIZMO	Co-Owner	4	1800	$130,000	8661	RELIGIOUS C	32.74818	-83.68601
GA	BEALLWOOD BAPTIST CHURCH	4650 VETERANS PARKWAY	COLUMBUS	31904	MUSCOGEE	7063222709	7063224091	CLARK STANDARD	Co-Owner	8	1920	$230,000	8661	RELIGIOUS C	32.54397	-85.01386
GA	GLENN ANTHONY BAPTIST CHURCH	1109 39TH STREET	COLUMBUS	31904	MUSCOGEE	7063222800	7063226822	UDELL ADDISON	Co-Owner	8	1945	$230,000	8661	RELIGIOUS C	32.54397	-85.01386
GA	GRACE BAPTIST CHURCH	2915 14TH AVENUE	COLUMBUS	31904	MUSCOGEE	7063231046	7063238554	DAVID PRICE	Co-Owner	4	1946	$130,000	8661	RELIGIOUS C	32.54397	-85.01386
GA	CARVER HIGH SCHOOL	3100 8TH ST	COLUMBUS	31906	MUSCOGEE	7066490689	7066494132	JOSEPH SAULSBUI	Co-Owner	150	1988	$210,000	8211	ELEMENTAR	32.46625	-84.95307
GA	COLUMBUS FIRST SDA SCHOOL	7880 SCHOMBURG RD	COLUMBUS	31907	MUSCOGEE	7065617601	7065617601	MOWA BRINKLEY	Co-Owner	1	1993	$19,000	8211	ELEMENTAR	32.47779	-84.82181
GA	ST MARY MAGDALENE EPISCOPAL CH	4244 SAINT MARYS ROAD	COLUMBUS	31907	MUSCOGEE	7066892790	7066894219	BENJAMIN SPEARE	Co-Owner	4	1984	$130,000	8661	RELIGIOUS C	32.47779	-84.82181
FL	STRASSER CONSTRUCTION CO	1030 N US HIGHWAY 1	ORMOND BEAC	32174	VOLUSIA	3866737007	3866737055	SCOTT STRASSER	Executive D	3	1957	$890,000	1521	GENERAL CI	29.29923	-81.1865
FL	AMERICAN REALTY OF FLORIDA	3076 GULF BREEZE PKWY	GULF BREEZE	32561	SANTA ROS	8509164499	8509164999	MARGARET MILLEF	Co-Owner	2	1997	$110,000	6531	REAL ESTAT	30.3556	-87.11058
FL	WEKIWA GARDENS, INC	496 N LAKE PLEASANT RD	APOPKA	32712	ORANGE	4078893000	4078893848	A KATHREIN MARK	Executive D	15	1970	$1,000,000	5261	RETAIL NUR	28.73141	-81.50703
FL	COMMUNITY COUNSELING CENTER AT	4851 S APOPKA VINELAND RD	ORLANDO	32819	ORANGE	4078764991	4078766495	WILLIAM S BARNES	Co-Owner	100	1979	$1,900,000	8661	RELIGIOUS C	28.45013	-81.47259
FL	INTERIOR WOODWORK, INC	240 W 27TH ST	HIALEAH	33010	MIAMI-DADE	3058879085	3058843902	HUMBERTO PANTA	Executive D	128	1976	$3,500,000	1751	CARPENTRY	25.8284	-80.28649
FL	SAMARI LAKES MANAGEMENT OFFICE	10000 NORTHWEST 80TH COURT	HIALEAH	33016	MIAMI-DADE	3055589154	3055589391	RAFAEL PENALVEI	Co-Owner	6	1984	$150,000	8641	CIVIC, SOCIA	25.89092	-80.3353
FL	GULF MANUFACTURING COMPANY	2450 NW 150TH ST	OPA LOCKA	33054	MIAMI-DADE	3056815550	3056815565	CLARA I GOMEZ	Executive D	6	1986	$560,000	3089	PLASTICS PI	25.90415	-80.25572
FL	CORAL VILLA CHRISTIAN ACADEMY	3201 SOUTHWEST 67TH AVENUE	MIAMI	33155	MIAMI-DADE	3056614998	3056621648	FE VILLANUEVA	Co-Owner	3	1976	$33,000	8351	CHILD DAY C	25.73652	-80.31089
FL	NAVAMA, INC	12303 SW 133RD CT	MIAMI	33186	MIAMI-DADE	3052597494	3052597502	CARLOS J NAVARI	Executive D	3	1996	$474,000	8711	ENGINEERIN	25.65603	-80.41486
FL	ST JOHN UNITED METHODIST CHURCH	1520 NW 5TH ST	FORT LAUDERI	33311	BROWARD	9544671692	9547678389	ANN DAVIS	Co-Owner	3	1946	$99,000	8661	RELIGIOUS C	26.14376	-80.17348
FL	VANCE BALDWIN, INC	7060 W STATE ROAD 84 STE 12	DAVIE	33317	BROWARD	9549691811	9549690226	ROBERT B COOLID	Executive D	82	1954	$9,900,000	5065	ELECTRONIC	26.11087	-80.22732
FL	MARLA PORTER GROSS	1689 OSPREY BND	WESTON	33327	BROWARD	9542176001	9543153471	MARLA PORTER GI	Co-Owner	2	2005	$51,000	8111	LEGAL SERV	26.11907	-80.41508
FL	EXOTIC COLLECTORS NURSERY INC	9470 158TH RD S	DELRAY BEAC	33446	PALM BEAC	5614997834	5614997858	PATRICIA MERCAD	Executive D	3	1978	$130,000	811	TIMBER TRA	26.45426	-80.18914
FL	IT'S A HAIRY BUSINESS	75 E INDIANTOWN RD	JUPITER	33477	PALM BEAC	5617489939	5617489942	RENEE WALKER	Co-Owner	1	1996	$18,000	7231	BEAUTY SH	26.91503	-80.07598
FL	TEMCO DRUGS INC	5909 SE ABSHIER BLVD	BELLEVIEW	34420	MARION	3522452214	3522452214	THERESA KISER	Executive D	7	1986	$530,000	5912	DRUG STOR	29.05136	-82.04049
AL	HAPPY CATERING CO	2021 3RD AVENUE NORTH	BIRMINGHAM	35203	JEFFERSON	2052518925	2059160077	RHONDA BOULOUI	Co-Owner	3	1992	$77,000	5812	RESTAURAN	33.51926	-86.80755
AL	HOLLYHAND DOUG CONSTRUCTION C	527 MAIN AVE STE A	NORTHPORT	35476	TUSCALOOS	2053450955	2057585605	JANE HOLLYHAND	Executive D	21	1972	$40,115,000	1799	SPECIAL TRA	33.22379	-87.61069
AL	LAZY M, INC	69 CLARK DR	RUSSELLVILLE	35654	FRANKLIN	2059934869	2563323327	DEBRA LYNN MAY	Executive D	48	1984	$680,000	5712	FURNITURE S	34.48232	-87.62307
AL	GRADY RALLS & SONS, INC	12364 BROOKLYN RD	EVERGREEN	36401	CONECUH	3345784000	2515784200	WILLODEAN RALLS	Executive D	25	1966	$3,671,285	1611	HIGHWAY A	31.49498	-86.91384
AR	PRAIRIELAKE BAPTIST CHURCH	2611 SOUTH INDIANA STREET	PINE BLUFF	71601	JEFFERSON	8705364268	8705364268	REV LEE WHITKER	Co-Owner	3	2002	$87,000	8211	ELEMENTAR	34.19686	-91.90493
AR	PARKS & ROTHWELL CPA	107 EAST 3RD AVENUE	CROSSETT	71635	ASHLEY	8703643803	8703647853	JOBIE JOHNSTON	Co-Owner	2	1986	$58,000	8721	ACCOUNTIN	33.14767	-92.00193

what's worth protecting

if i stole this, what could i do with it?

Quarterly (in millions except per share amounts, unaudited)	2010 First Quarter	2010 Second Quarter	2010 Third Quarter	2010 Fourth Quarter	2009 First Quarter	2009 Second Quarter	2009 Third Quarter	2009 Fourth Quarter
Net revenue	$9,368	$14,801	$15,514	$18,155	$8,263	$10,592	$11,080	$13,297
Gross profit	$4,905	$ 8,056	$ 8,506	$ 9,796	$4,519	$ 5,711	$ 5,899	$ 7,004
Mark-to-market net impact[a]	$ (46)	$ 4	$ (16)	$ (33)	$ (62)	$ (100)	$ (29)	$ (83)
Merger and integration charges[b]	$ 321	$ 155	$ 69	$ 263	–	–	$ 9	$ 52
Gain on previously held equity interests[c]	$ (958)	–	–	–				
Inventory fair value adjustments[d]	$ 281	$ 76	$ 17	$ 24				
Venezuela currency devaluation[e]	$ 120	–	–	–				
Asset write-off[f]	$ 145	–	–	–				
Foundation contribution[g]	$ 100	–	–	–				
Debt repurchase[h]	–	–	–	$ 178				
Restructuring and impairment charges[i]					$ 25	$ 11	–	–
Net income attributable to PepsiCo	$1,430	$ 1,603	$ 1,922	$ 1,365	$1,135	$ 1,660	$ 1,717	$ 1,434
Net income attributable to PepsiCo per common share – basic	$ 0.90	$ 1.00	$ 1.21	$ 0.86	$ 0.73	$ 1.06	$ 1.10	$ 0.92
Net income attributable to PepsiCo per common share – diluted	$ 0.89	$ 0.98	$ 1.19	$ 0.85	$ 0.72	$ 1.06	$ 1.09	$ 0.90
Cash dividends declared per common share	$ 0.45	$ 0.48	$ 0.48	$ 0.48	$0.425	$ 0.45	$ 0.45	$ 0.45
Stock price per share[j]								
High	$66.98	$ 67.61	$ 66.83	$ 68.11	$56.93	$ 56.95	$ 59.64	$ 64.48
Low	$58.75	$ 61.04	$ 60.32	$ 63.43	$43.78	$ 47.50	$ 52.11	$ 57.33
Close	$66.56	$ 63.56	$ 65.57	$ 65.69	$50.02	$ 53.65	$ 57.54	$ 60.96

(a) In 2010, we recognized $91 million ($58 million after-tax or $0.04 per share) of mark-to-market net gains on commodity hedges in corporate unallocated expenses. In 2009, we recognized $274 million ($173 million after-tax or $0.11 per share) of mark-to-market net gains on commodity hedges in corporate unallocated expenses.

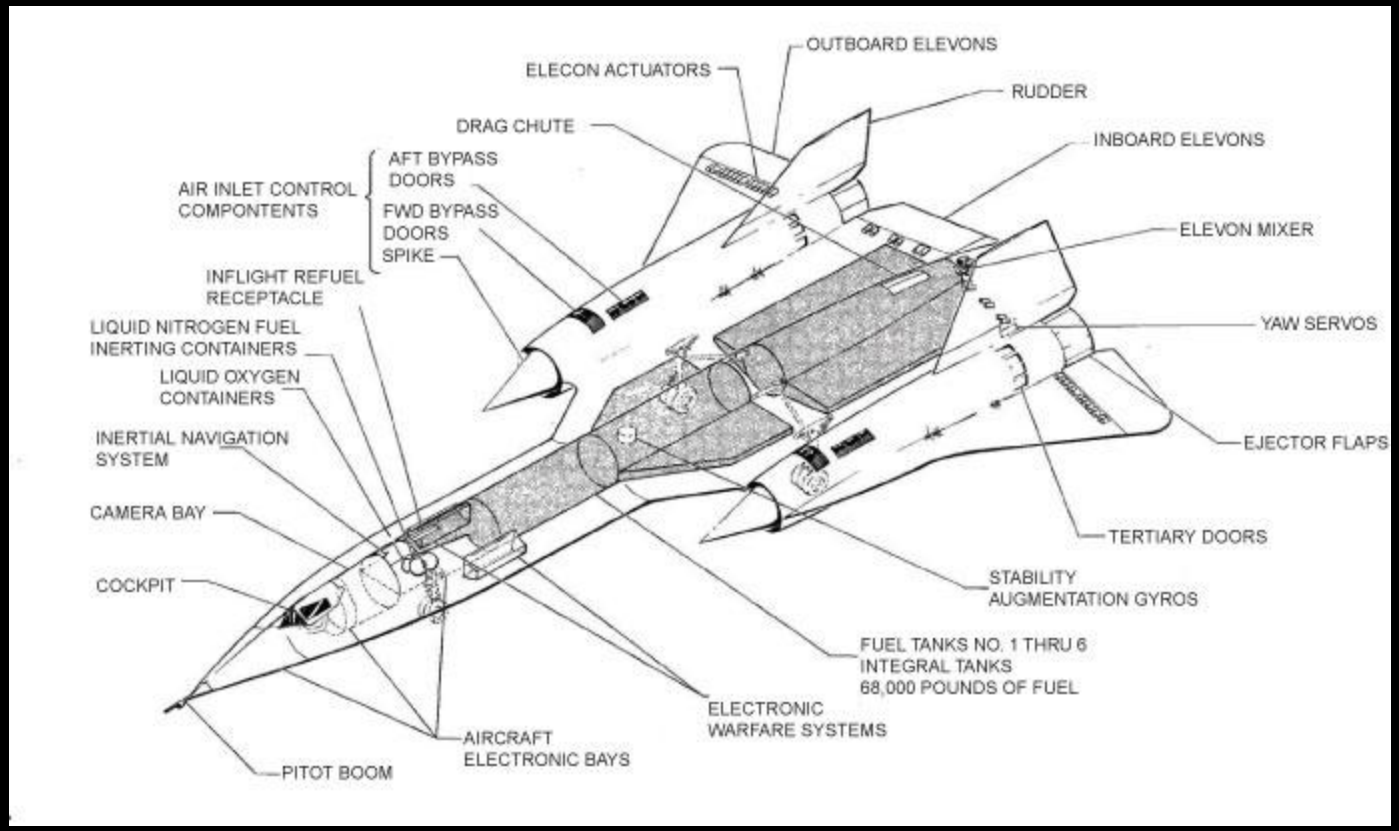
(b) In 2010, we incurred merger and integration charges of $799 million related to our acquisitions of PBG and PAS, as well as advisory fees in connection with our acquisition of WBD. In addition, we recorded $9 million of merger-related charges, representing our share of the respective merger costs of PBG and PAS. In total, these charges had an after-tax impact of $648 million or $0.40 per share. In 2009, we recognized $50 million of merger-related charges, as well as an additional $11 million of costs in bottling equity income representing our share of the respective merger costs of PBG and PAS. In total, these costs had an after-tax impact of

what's worth protecting

if i stole this, what could i do with it?

what's worth protecting

if i stole this, what could i do with it?



what are we up to

- why security matters
- what's worth protecting
- **principles of security**
- common exploits
- security resources

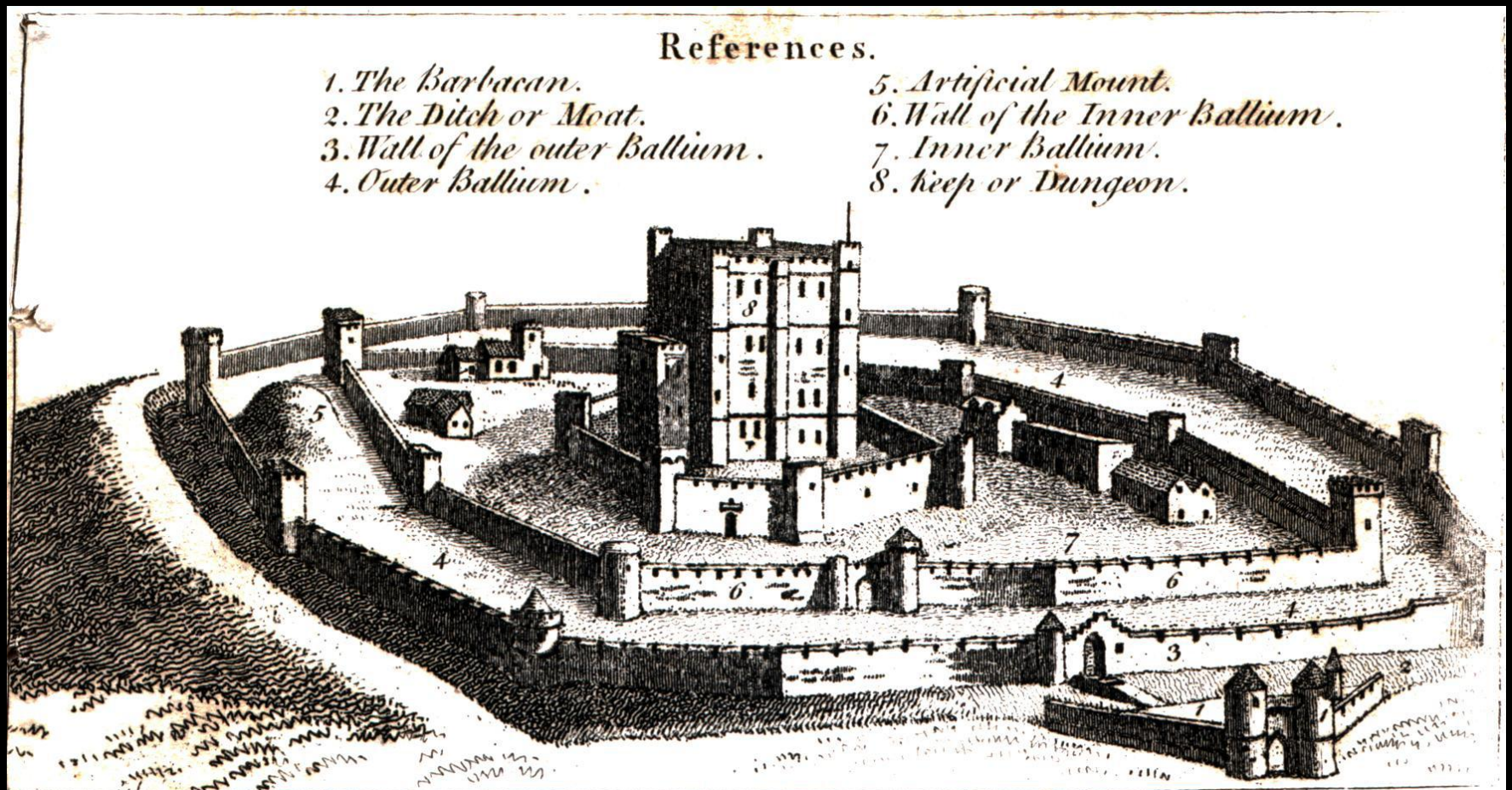
principles of security

DEFENSE-IN-DEPTH

The **ONION** Approach

principles of security

defense-in-depth



principles of security

defense-in-depth

principles of security

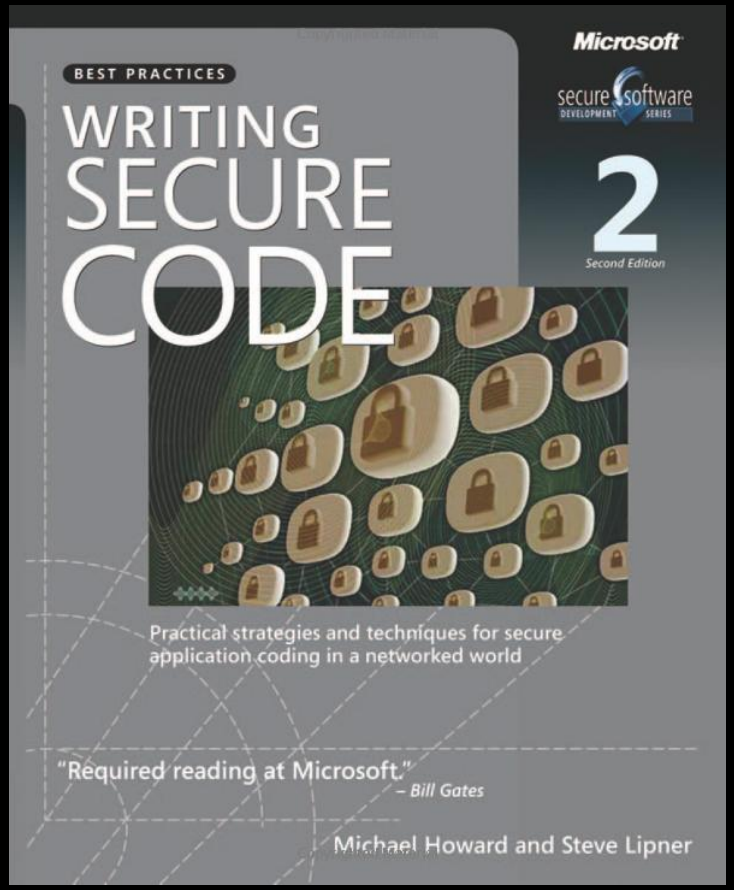
defense-in-depth

the principle of defense-in-depth is that layered security mechanisms increase security of the systems as a whole. if an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system

principles of security

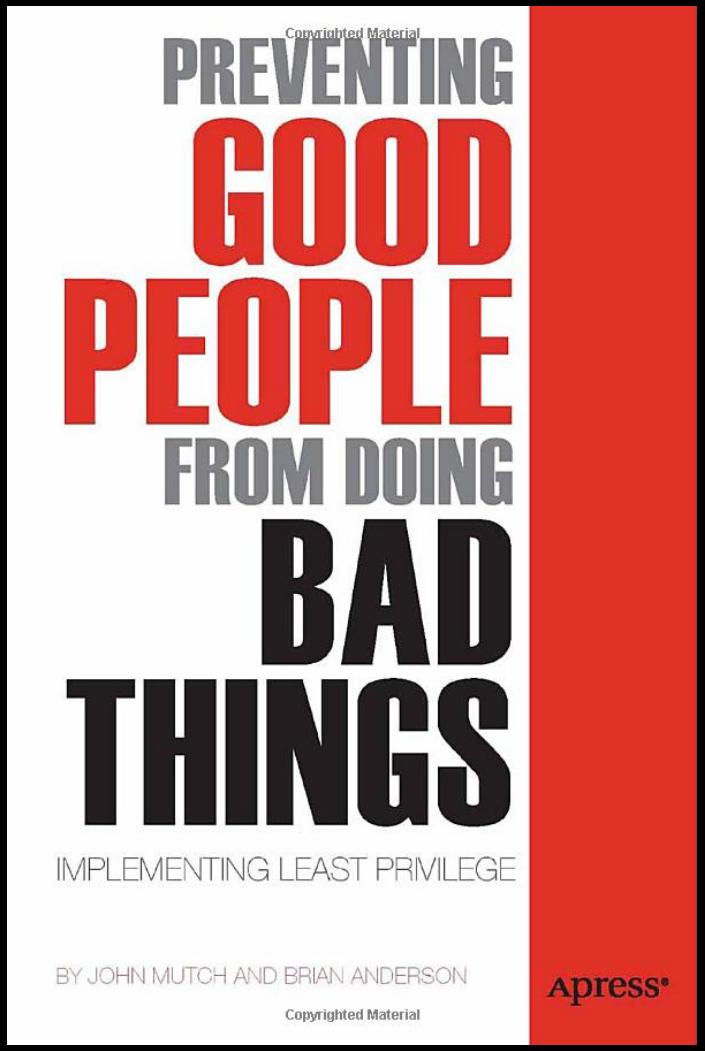
defense-in-depth

defense in depth is a straightforward principle: imagine your application in the last component standing and every defensive mechanism protecting you has been destroyed. now you must protect yourself. for example, if you expect a firewall to protect you, build the system as though the firewall has been compromised.



principles of security

least privilege



principles of security

least privilege

principles of security

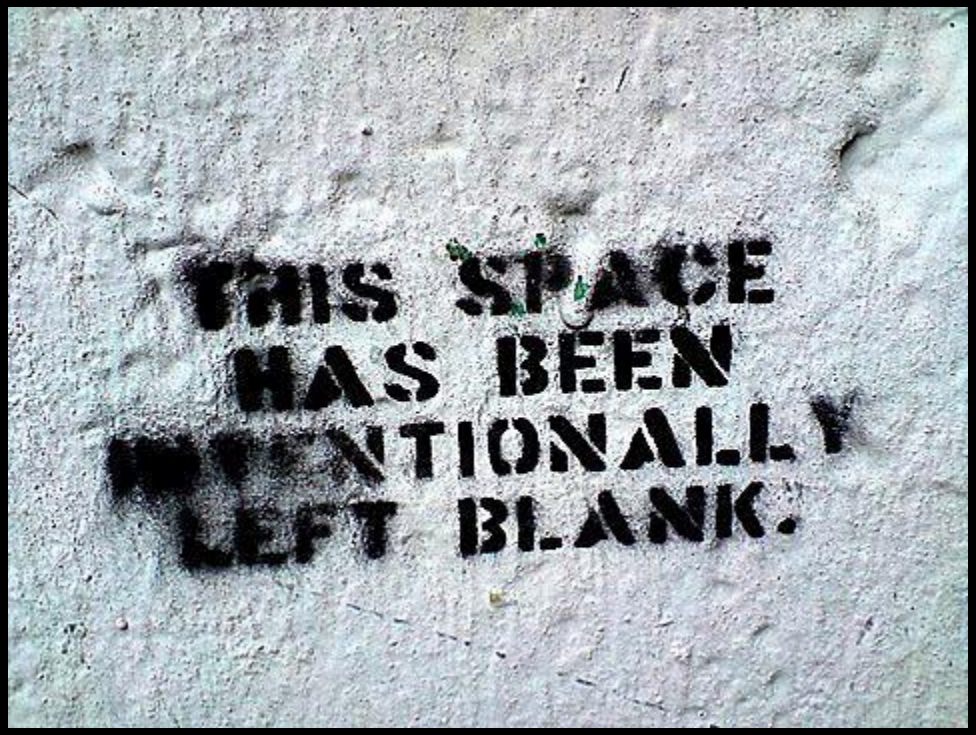
least privilege

a user or website must only be able to access information and resources necessary for its legitimate purpose

if bob in sales can't access credit card numbers, then the cards are safe if bob's password is stolen

principles of security

attack surface reduction



principles of security

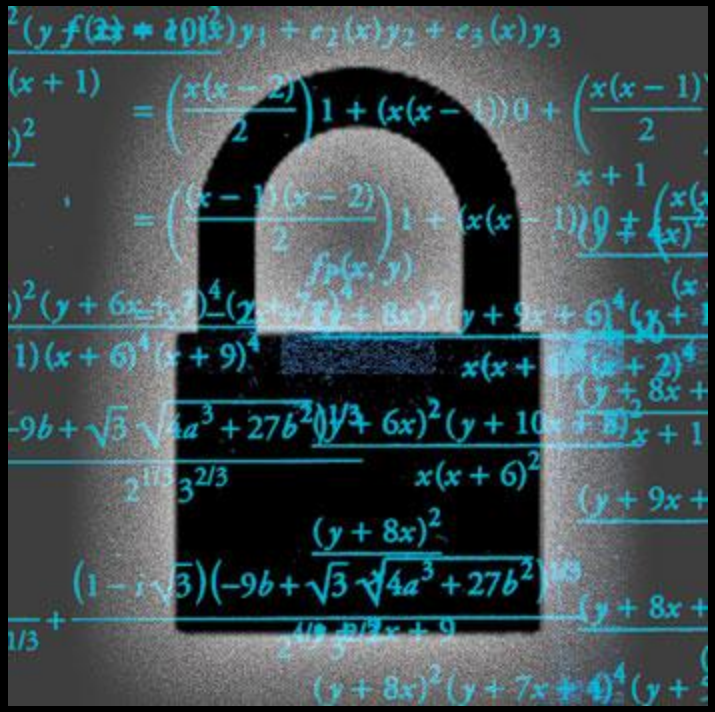
attack surface reduction

every feature of a website is a potential *surface* a hacker can try to attack.

the basic strategies of attack surface reduction are to reduce the amount of code running, reduce entry points available to untrusted users, reduce privilege levels as much as possible, and eliminate services requested by relatively few users.

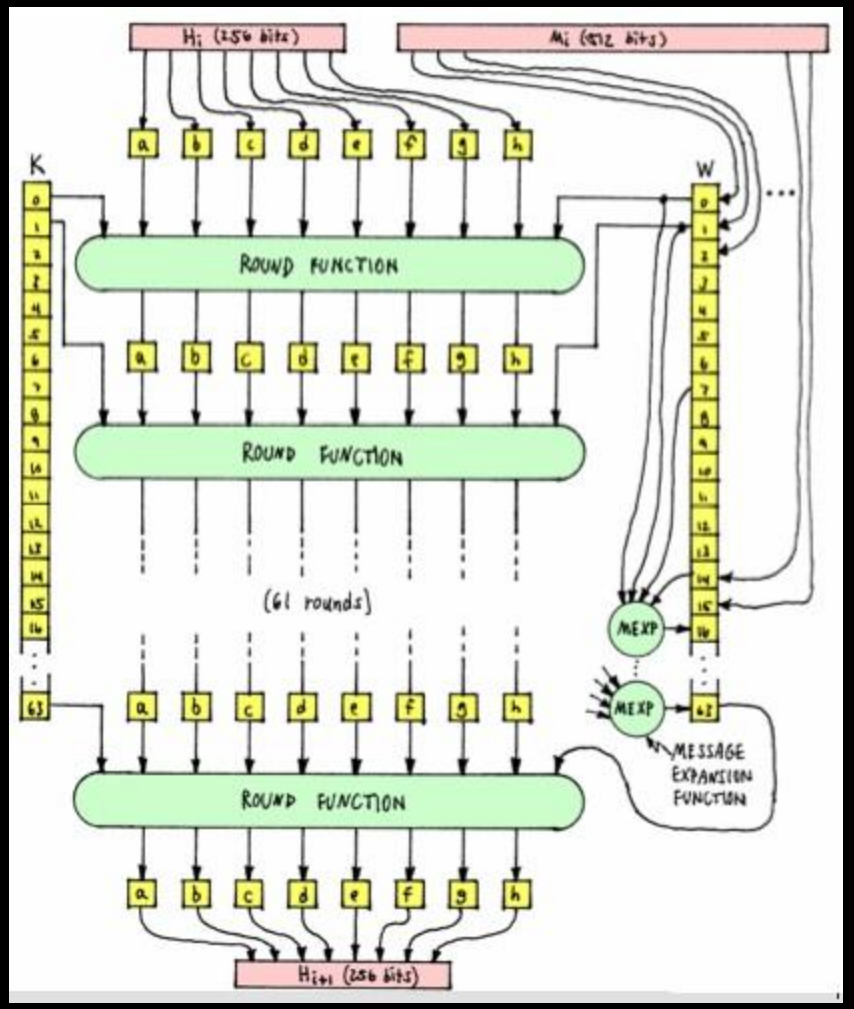
principles of security

cryptography is hard



principles of security

cryptography is hard



principles of security

cryptography is hard

- proper use of crypto is hard to do right
- experts frequently apply crypto incorrectly
- never write your own crypto
- there's a lot of snake oil out there

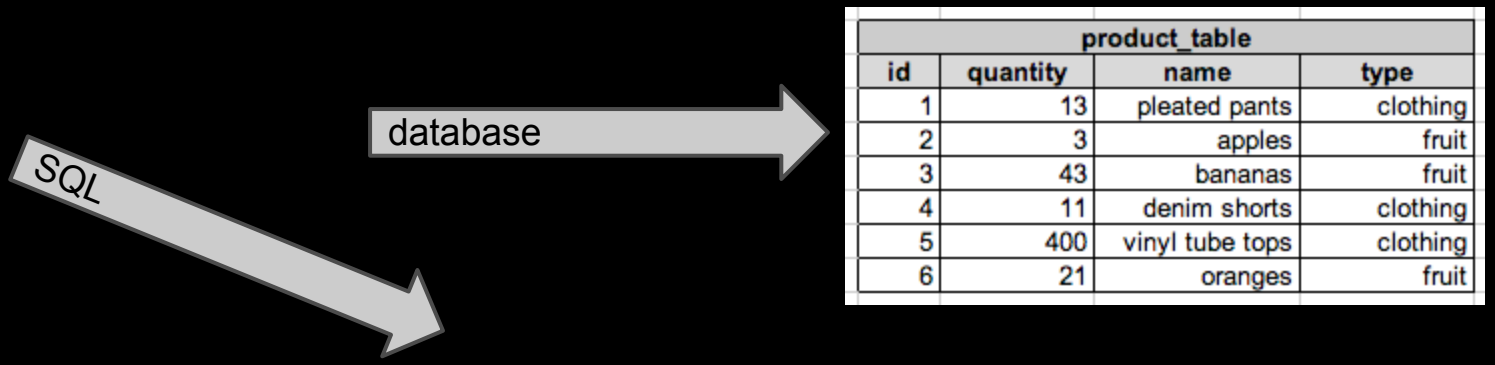
what are we up to

- why security matters
- what's worth protecting
- principles of security
- **common exploits**
- security resources

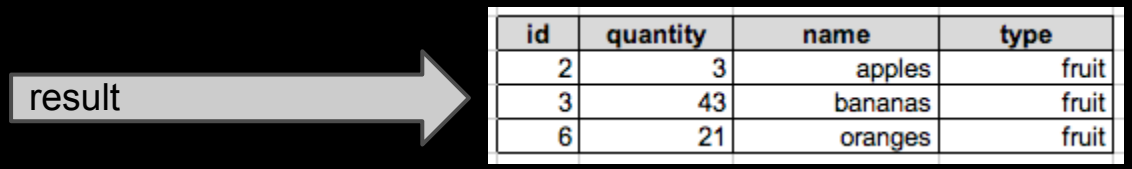
common exploits

SQL injection

Structure **Q**uery **L**anguage is the command set generally used to get data out of a database.




```
SELECT * FROM product_table WHERE type='fruit'
```



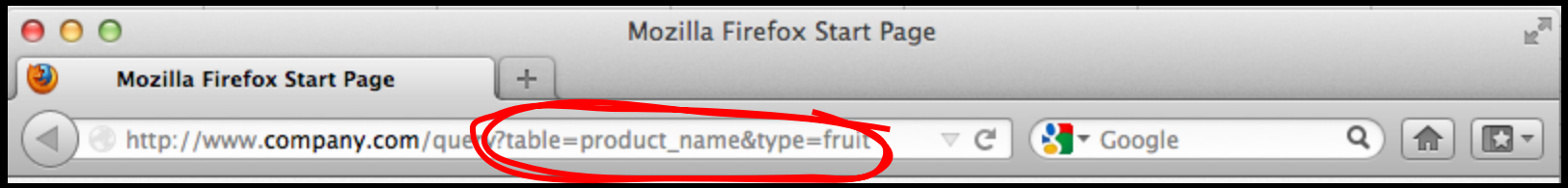
common exploits

SQL injection

database has 2 tables

product_table			
id	quantity	name	type
1	13	pleated pants	clothing
2	3	apples	fruit
3	43	bananas	fruit
4	11	denim shorts	clothing
5	400	vinyl tube tops	clothing
6	21	oranges	fruit

users				
id	name	email	ssn	type
1	Joe	joe@gmail.com	158-73-0467	admin
2	Jane	jane@gmail.com	201-53-4956	admin
3	Jim	jim@spam.com	867-53-0943	customer
4	John	john93@aol.com	301-86-8675	customer
5	Jennie	super_tony@pow.org	143-10-0303	customer
6	Jacob	timtim@nero.gov	697-24-4202	customer




```
"SELECT * FROM" + request['table'] + "WHERE type=" +
request['type']
```

result

id	quantity	name	type
2	3	apples	fruit
3	43	bananas	fruit
6	21	oranges	fruit

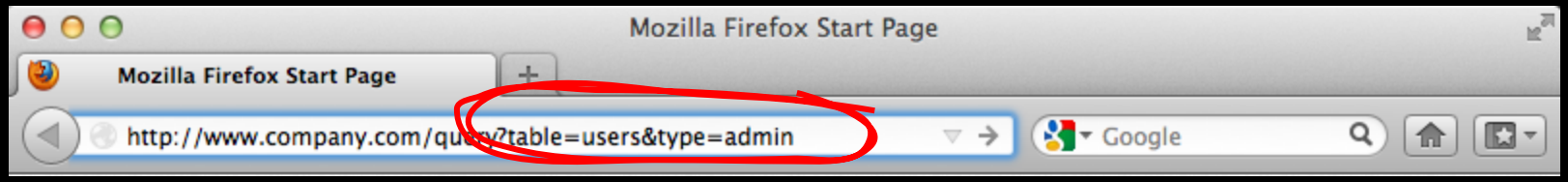
common exploits

SQL injection

database has 2 tables

product_table			
id	quantity	name	type
1	13	pleated pants	clothing
2	3	apples	fruit
3	43	bananas	fruit
4	11	denim shorts	clothing
5	400	vinyl tube tops	clothing
6	21	oranges	fruit

users				
id	name	email	ssn	type
1	Joe	joe@gmail.com	158-73-0467	admin
2	Jane	jane@gmail.com	201-53-4956	admin
3	Jim	jim@spam.com	867-53-0943	customer
4	John	john93@aol.com	301-86-8675	customer
5	Jennie	super_tony@pow.org	143-10-0303	customer
6	Jacob	timtim@nero.gov	697-24-4202	customer




```
"SELECT * FROM" + request['table'] + "WHERE type=" +
request['type']
```

result

id	name	email	ssn	type
1	Joe	joe@gmail.com	158-73-0467	admin
2	Jane	jane@gmail.com	201-53-4956	admin

common exploits

SQL injection

SQL injection is an exploit where a SQL query is built using input from the user. the attacker sends specific input that causes the website to show, edit, or destroy unintended information in the database.

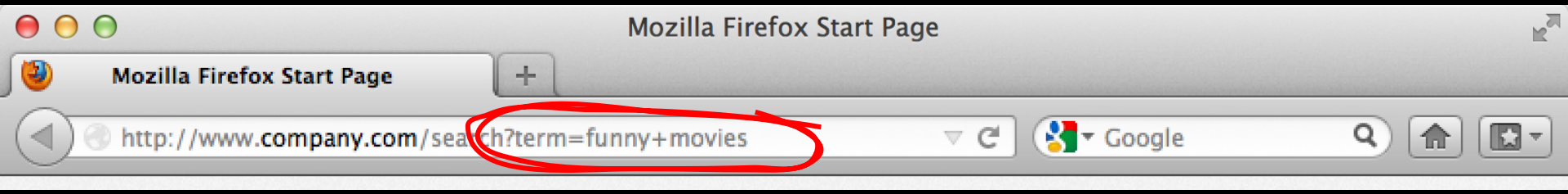
common exploits

protecting against SQL injection

- never write *raw SQL* in your web code instead use a library for accessing the database that explicitly protects against SQL injection
- libraries make use of things like *prepared statements* and *query escaping*
- use *active proxy* tools like *rat proxy* or *burp proxy* to test for SQL injection on your site
- apply defense-in-depth

common exploits

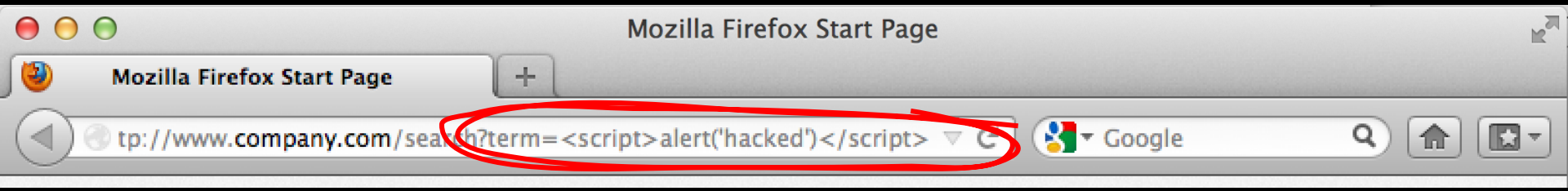
XSS - cross site scripting




```
<title>search for stuff</title>
<body>
    <h1>searching for {{ term }}</h1>
    <ul>
    {% for result in search_results %}
        <li><a href="{{ results.url }}">{{ result.name }}</a></li>
    {% endfor %}
    </ul>
</body>
```

common exploits

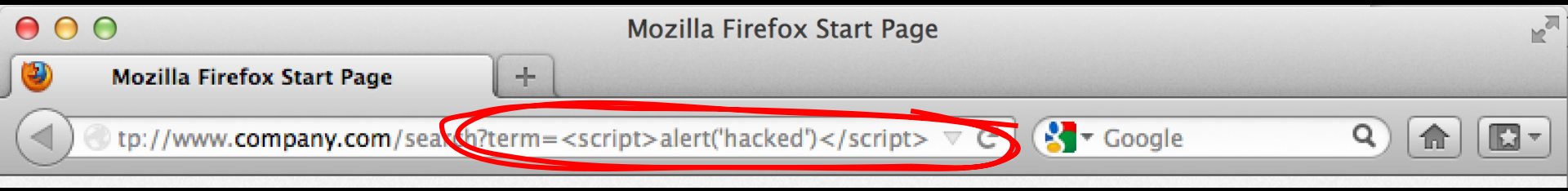
XSS - cross site scripting




```
<title>search for stuff</title>
<body>
    <h1>searching for {{ term }}</h1>
    <ul>
    {% for result in search_results %}
        <li><a href="{{ results.url }}">{{ result.name }}</a></li>
    {% endfor %}
    </ul>
</body>
```

common exploits

XSS - cross site scripting




```
<title>search for stuff</title>
<body>
    <h1>searching for <script>alert('hacked')</script></h1>
    <ul>
    </ul>
</body>
```

common exploits

XSS - cross site scripting

XSS is an exploit where a page displays user input. the attacker sends specific input that causes the website to unintentionally run malicious javascript.

- *reflected XSS* - user input is echoed back right away
- *stored XSS* - user input is stored in a database and then shown on a different page

common exploits

protecting against XSS

character	escape sequence
<	<
>	>
"	"
&	&

html allows for special characters like < or > to be represented with an *escape sequence*. the escape sequence can't trick a browser into running a <script> tag where one wasn't intended.

- always validate input as soon as it is received
- always escape output before sending to the user

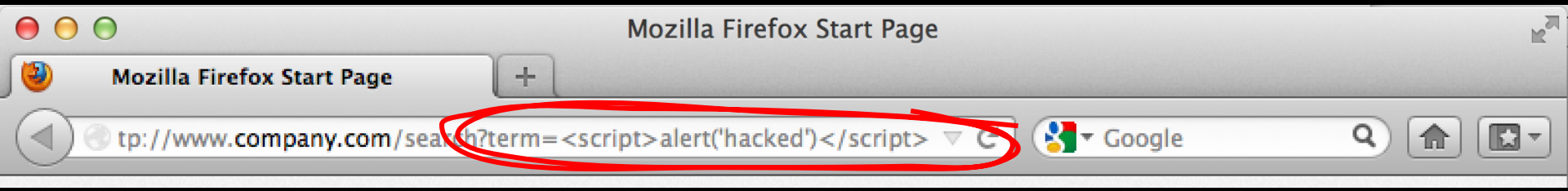
common exploits

protecting against XSS

- html template systems like jinja2 or django provide automatic escaping on output
- use *active proxy* tools like *rat proxy* or *burp proxy* to test for XSS on your site
- apply the principle of defense-in-depth: check input on the client with javascript, check input again on the server, then check output

common exploits

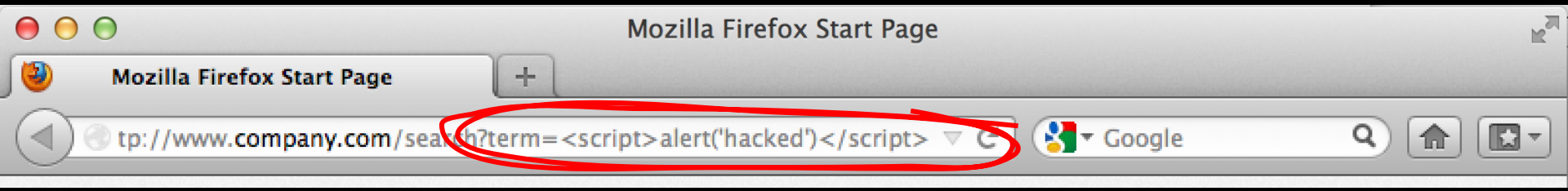
protecting against XSS




```
<title>search for stuff</title>
<body>
    <h1>searching for {{ html_escape(term) }}</h1>
    <ul>
    {% for result in search_results %}
        <li><a href="{{ results.url }}">{{ result.name }}</a></li>
    {% endfor %}
    </ul>
</body>
```

common exploits

protecting against XSS

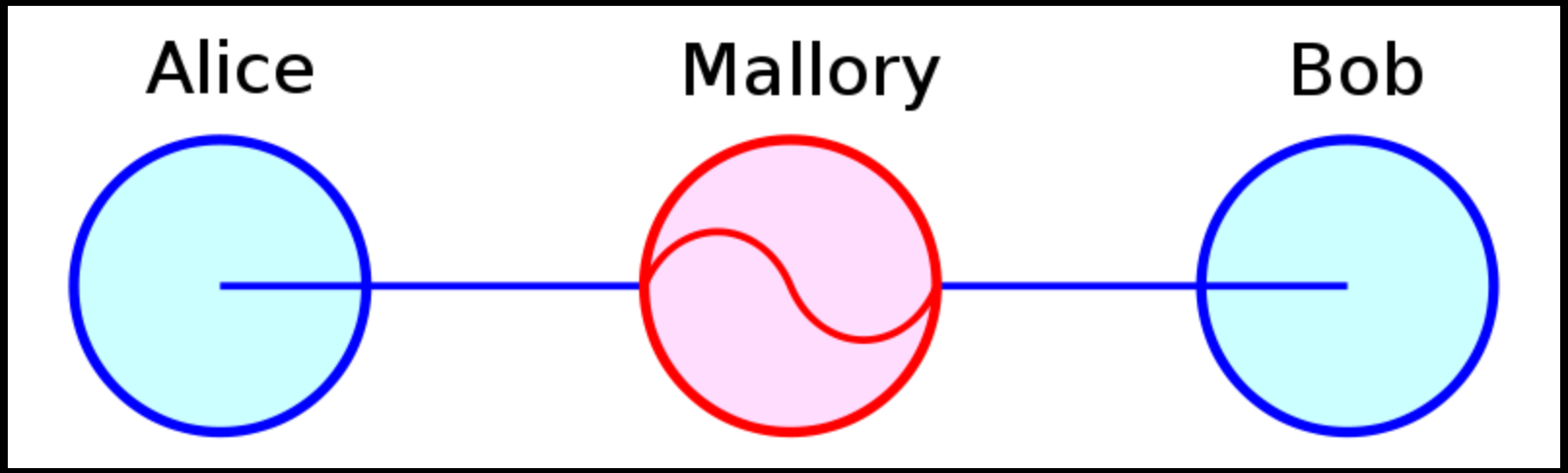



```
<title>search for stuff</title>
<body>
    <h1>searching for  &lt;script&gt;alert('hacked')&lt;/script&gt;</h1>
    <ul>
    </ul>
</body>
```

common exploits

man-in-the-middle

when pages show sensitive data but don't use https, then an attacker can spy on the sensitive data. this spying is called *man-in-the-middle*.



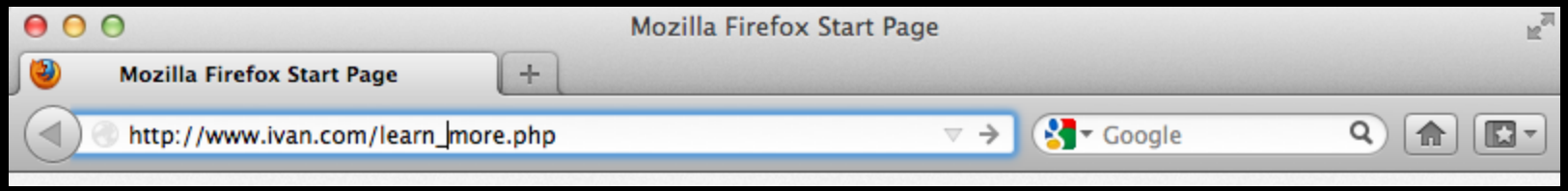
common exploits

protecting against man-in-the-middle

- design your site to only transmit sensitive data over https. adding https late makes design hard
- never mix https and http images, scripts, or other resources on the same page
- make sure your SSL certificate is valid
- apply the principle of attack surface reduction. the less sensitive data you show, the better

common exploits

CSRF - cross site referral forgery

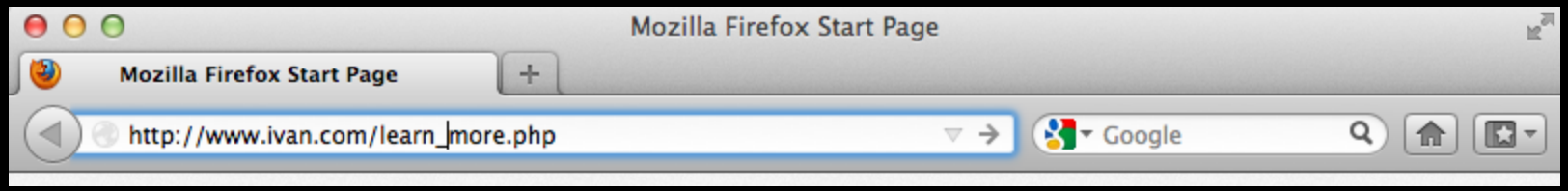



```
<title>learn more about ivan.com</title>
<body>
    <h1>ivan is i   lly interesting</h1>
    <a href="https://www.gmail.com/delete_all">
        click here to learn more!!
    </a>
</body>
```

whoa! unexpected!

common exploits

CSRF - cross site referral forgery




```
<title>see my awesome photo</title>
<body>
    <h1>photos are cat</h1>
    <img src="https://www.gmail.com/delete_all">
        see a pretty photo!!
</body>
```

that's no image!

common exploits

CSRF - cross site referral forgery

CSRF forces a user to visit a page for which he/she is already authenticated. the user ends up execute actions of the attacker's choosing. a successful CSRF exploit can compromise end user data and operation in case of normal user. attacks targeting an administrator account, can compromise an entire site.

common exploits

protecting against CSRF

- require that sensitive actions use an http POST - a form - rather than a GET - a simple link
- use a framework like django or jinja which has built in CSRF protection for form POST
  - forms include a hidden field with a secret value that has to be submitted with the form
  - CSRF tokens are tied to a specific user and pageview
  - attackers can not guess what *magic* token should go with a specific

common exploits

protecting against CSRF

```
<form method="post" action="/delete_all">
    <input type="hidden"
           name="csrf_token"
           value="jBGh345Tls98" />
    <input type="submit"
           value="delete your mail" />
</form>
```

common exploits

social engineering

social engineering is manipulating people into divulging confidential information like passwords, private website addresses, information on how data is stored, etc.

there are few technical solutions to social engineering but user education, policies, and good use of security principles help mitigate.

what are we up to

- why security matters
- what's worth protecting
- principles of security
- common exploits
- **security resources**

security resources

OWASP
Open **W**eb **A**pplication **S**ecurity **P**roject

https://www.owasp.org

tons more information on all these topics

security resources

CWE
Common **W**eakness **E**numeration

http://cwe.mitre.org

tons more information on all these topics

security resources

reddit
/r/netsec

http://www.reddit.com/r/netsec

topical discussion among professionals and wannabees